4-2018

A Survey of Security and Privacy in Mobile Cloud Computing

Bhuvaneswari Rayapuri
Western Michigan University

A Survey of Security and Privacy in Mobile Cloud Computing

by

Bhuvaneswari Rayapuri

A thesis submitted to the Graduate College
in partial fulfillment of the requirements
for the degree of Master of Science
Computer Science
Western Michigan University
April 2018

Thesis Committee:

Dr. Leszek T. Lilien, Ph.D., Chair
Dr. Ikhlas Abdel-Qader, Ph.D.
Dr. Seung-Hee Bae, Ph.D.

A Survey of Security and Privacy in Mobile Cloud Computing

Bhuvaneswari Rayapuri, M.S.

Western Michigan University, 2018

Cloud Computing is an emerging technology that provides shared processing resources and data to computers and other devices on demand. On the other hand, Mobile Computing allows transmission of data, voice and video. From these two there emerges a new concept Mobile Cloud Computing which not only overcomes the problems of Mobile Computing but also integrates Cloud Computing into Mobile Environments to overcome obstacles related to Performance, Security and Environment. This paper also provides a decent description on Security and Privacy, its related problems, threats and challenges. This paper first provides details on survey of Mobile Cloud Computing, then it talks about Architecture, Application, Security and Privacy in Mobile Cloud Computing, Intertwined Security and Privacy in Mobile Cloud Computing and finally ends with Conclusion and Future work.

ACKNOWLEDGMENTS

I would first like to thank my parents and to my brother for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

I would like to thank my thesis advisor Dr. Leszek Lilien. The door to Prof. Lilien office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right direction whenever he thought I needed it.

I would also like to thank the experts: Dr. Ikhlas Abdel-Qader (Professor of Electrical and Computer Engineering) and Dr. Seung-Hee Bae (Professor of Computer Science) who were involved in the validation survey for this research project. Without their passionate participation and input, the validation survey could not have been successfully conducted.

Finally, I must express my very profound gratitude to god for giving me a life to make it worthy.

Bhuvaneswari Rayapuri

TABLE OF CONTENTS

Table of Contents—Continued

Table of Contents—Continued

LIST OF TABLES

LIST OF FIGURES

List of Figures--Continued

1. INTRODUCTION

This section starts with defining Cloud Computing (CC), then gives an overview of Mobile Cloud Computing (MCC), later defines security and privacy and ends with survey organization.

1.1. Definition of Cloud Computing (CC)

Cloud Computing (CC) is a coalesce of many computing fields and has gained much popularity in recent years (since 2007) [Khan et al., 2014b]. There is no consensual description on what a Cloud Computing or a Cloud Computing system is; dozens of developers and organizations describe it from different perspectives [Qi et al., 2012,]. Before describing it, we need to know what Cloud Computing is, "A kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand [Cloud Computing, Wikipedia, 2017]." It has three main benefits for businesses and end users: (i) self-service provisioning; (ii) elasticity; and (iii) pay per use [Mell and Grace, 2009].

The Cloud Computing services are a part of service model (which are included in Cloud Computing architecture) and these services can be private, public or hybrid [Cloud Computing, Wikipedia, 2017; NEC Company Ltd. and Information and Privacy commissioner, 2010] as shown in Figure 1:

1) *Private Cloud*—It refers to Cloud Computing on private network, where the cloud is exclusively built for one client and is managed by company's own cloud provider or IT organization.
2) *Public Cloud*—This cloud is for external users who can register with cloud on pay-per-use basis and can use the cloud resources accordingly. This cloud is not as secured as private cloud as it is accessible to internet users.
3) *Hybrid Cloud*—It is a combination of public and private cloud models, which determines how to distribute application across both public and private cloud.

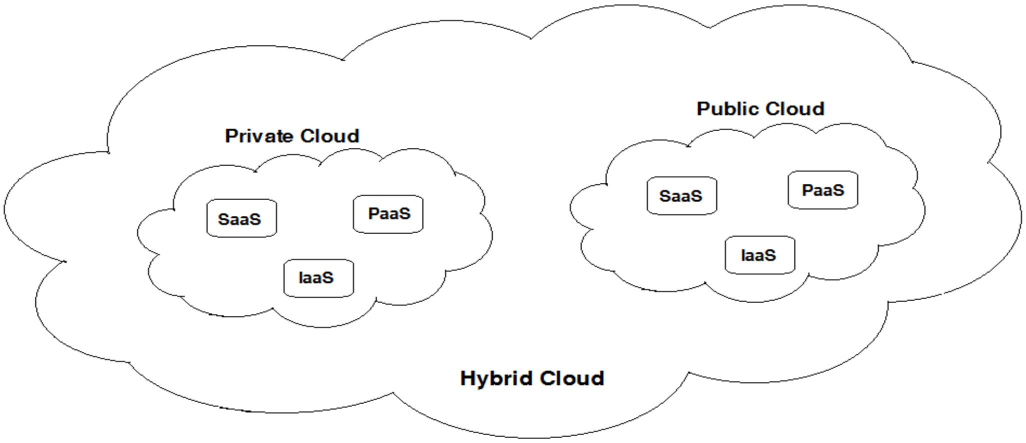


Figure 1. Three Types of Cloud Computing Deployment Models [cf. (Cloud Computing, Wikipedia, 2016)].

Figure 1, shows three types of CC services. In each service, there are three service types (which are categories of CC services), SaaS, PaaS, IaaS [Dinh et al., 2011]:

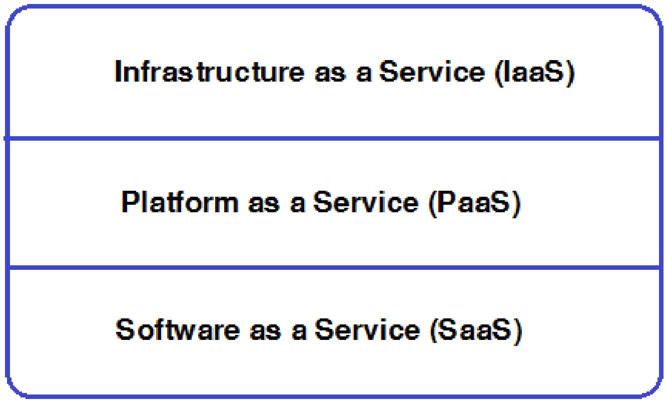

Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)

Figure 2. Service-Oriented Cloud Computing Architecture [cf. (Dinh et al., 2011)].

1) *Infrastructure as a Service (IaaS)*—IaaS enables the provision of storage, network, servers, and networking components to the users. The consumers can deploy and run arbitrary software's (OS, application, etc.) using these provisions [Cloud Computing, Wikipedia, 2017].

   Examples: Amazon Elastic Cloud Computing (EC2) and Simple Storage Services (S3) [Amazon Simple Storage Service details, Wikipedia, 2016].

2) *Platform as a Service (PaaS)*—PaaS provides Application Programming Interface (API's) models, programming environments and advanced integrated environment for building, testing, and deploying custom application.
   Examples: Google App Engine, Microsoft Azure, Amazon Map Reduce / S3.

3) *Software as a Service (SaaS)*—SaaS supports software distribution with specific requirements. It runs on pay-per-use basis, where the user can pay to access the information and application (via Internet) according to the use.
   Examples: Microsoft Office 365, Salesforce, Microsoft's Live Mesh, etc.

Cloud Computing allow customers to rent computation and storage such that customers can start instances of their cloud application as Virtual Machines (VM). In addition to this, cloud providers provide services such as backup, traffic accounting (to manage Virtual Machine instances with ease), CPU time, memory usage, storage, server availability, networking throughput, etc., to their customers. In order to reduce network latency, some cloud providers offer their customers to choose a geographically nearby data center to run their VM instances, example of one such cloud provider is Amazon. This kind of Cloud Computing is suitable and popular for small startups and medium-sized business, but it still needs to be proven for large organization as each large company must investigate price and performance trade-off between building and managing their own private cloud or leasing third party's cloud. A key consideration is whether an organization stores its private or proprietary data on third party's cloud and if it does, to what extent protection is ensured to that data. The future of the cloud is envisioned where large companies can build their own private cloud [Bahl et al., 2012].

Cloud Computing includes: Fog, Edge, Mist Computing, etc.:

1) *Fog Computing*—It refers to extending cloud computing to the edge of an enterprise's network. It facilitates the operation of compute, storage, and networking services between end devices and cloud computing data centers [Jonathan, 2013].
2) *Edge Computing*—A method of optimizing cloud computing systems by performing data processing at the edge of the network, near the source of the data [Lopez et al., 2015].
3) *Mist Computing*—A lightweight and rudimentary form of computing power that resides directly within the network fabric at the extreme edge of the network fabric using microcomputers and microcontrollers to feed into Fog Computing nodes and potentially onward towards the Cloud Computing platforms [Jones, 2017].

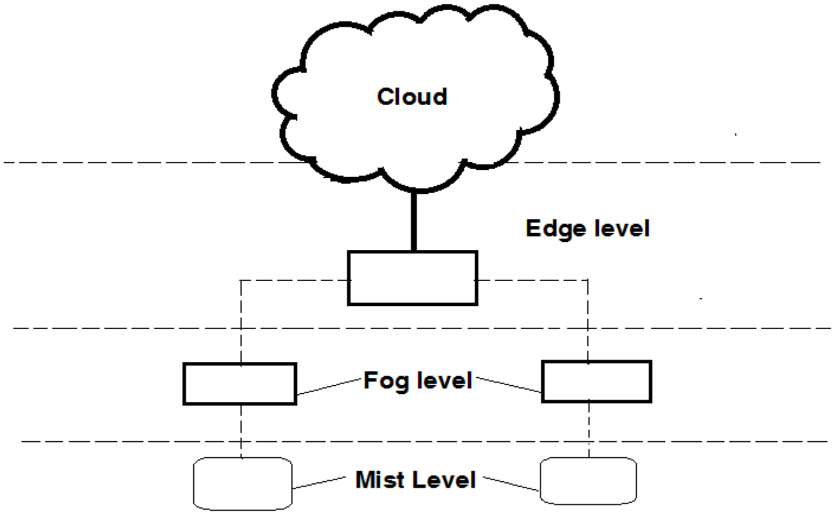


Figure 3. Cloud to Mist [cf. (Jones, 2017)].

Cloud Computing plays a major role in modern technology. Apart from Pc’s and Laptops, today’s mobile applications has also begun to adapt Cloud Computing, which has paved a way for a new concept called Mobile Cloud Computing, a combination of Cloud Computing and Mobile Computing (MC) (which requires rethinking in architecture of CC to accommodate common themes of MC) [Dinh et al., 2011].

1.2. Overview of Mobile Cloud Computing (MCC)

This section deals with defining Mobile Computing (MC), Mobile Cloud Computing (MCC). Later it discusses about the advantages and disadvantages of MCC.

1.2.1. Mobile Computing (MC)

"It is a human–computer interaction by which a computer is expected to be transported during normal usage, which allows for transmission of data, voice and video. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc networks and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications [Mobile Computing (Wikipedia), 2017]."

Features of MC [Qi et al., 2012]**.** The Features of MCC are as follows:

1) *Mobility*—Mobile nodes are free to establish connection with other nodes (even if they are fixed, in wired networks) during their free movement through Mobile Support Station (MSS).

Challenges of MC [Qi et al., 2012]**.** When compared to wired environments, wireless networks (like MC) face various issues like limited power, handoff delay, security, low computing ability, and so on, due to numerous mobile nodes and environment. Apart from this the Quality of Service (QoS) in mobile computing network is much easily affected by land forms, weather, buildings, etc.

Limitations of MC [Redekar et al., 2014]**.** The following are the limitations of MC:

1) *Insufficient Bandwidth*—Mobile Internet access is slower than direct cable connections. New technologies like 3G, 4G, etc., would not make much difference in the bandwidth (it is insufficient), even high speed wireless LANs are slower (than direct cable connection) due to limited range.
2) *Security Standards*—User should while using public networks in their mobile devices, as the Virtual Private network (VPN) is easily attacked. So, security becomes a major concern while using mobile devices.
3) *Power Consumption*—Mobile devices do not depend on battery power unlike desktop, laptop, etc. To obtain necessary battery life one has to use expensive batteries (in their mobile devices). To overcome this problem MC should look into greener IT to save power or increase battery life.
4) *Transmission Interference*—There may be a lot of interferences in signal transmission between mobile nodes, this can be due to weather or range from nearest signal point. Tunnels, buildings, rural, and forest areas have very less signal reception.
5) *Frequent Disconnection*—Due to some limitations in mobile devices like battery power, network conditions, etc., mobile nodes may not maintain the connection in a consistent way.

6) *Dis-Symmetrical Network Communication*—Even though the network used in mobile nodes are not any different, the communication between servers and access points are not symmetrical, as the mobile nodes have weak send/receive ability.
7) *Low reliability*—To address security issues, mobile computing network system has to be considered from terminals, data base platforms, and application development as the signals (inside the network system) are susceptible to interference and snooping.

1.2.2. Motivation of Mobile Cloud Computing (MCC)

Cloud Computing propels a new class of applications by extending Mobile Cloud application with unlimited storage, computation resource and task oriented service called Mobile Cloud Computing (MCC). Figure 3, describes MCC, where Mobile Cloud Computing integrates Cloud Computing, Mobile Computing, and wireless networks to bring rich computational resources to mobile users, network operators as well as Cloud Computing providers [Mobile Cloud Computing, Wikipedia, 2017].

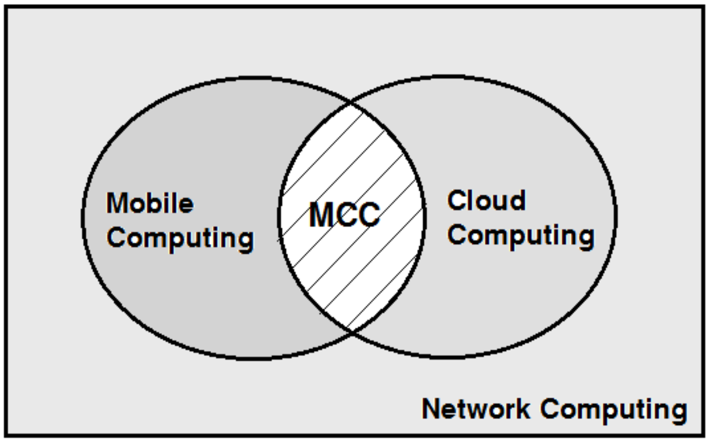


Figure 4. Foundation of MCC [cf. (Chang et al., 2013)]

More comprehensively, MCC is defined as a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies towards unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle [Sanaei et al., 2013].

In another definition, Mobile Cloud Computing is defined as the availability of Cloud Computing services in a mobile ecosystem [Cox, 2011].

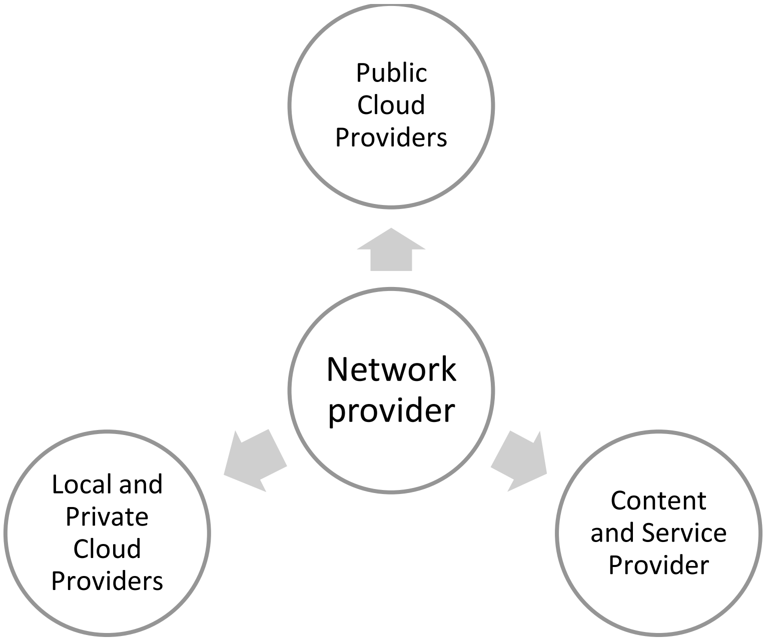

Public Cloud Providers
Network provider
Local and Private Cloud Providers
Content and Service Provider

Figure 5. MCC Ecosystem (cf. [Rahimi et al., 2014]).

Figure 4 illustrates general ecosystem of Mobile Cloud Computing and some of its components [Rahimi et al., 2014]:

1) *Network Providers*—They provide network infrastructures to all MCC components to communicate with each other.
2) *Public Cloud providers*—Storage facilities and high computations are made available to the public (via Internet). These computations and storage facilities are scalable and elastic.
3) *Content and Service providers*—They are neither scalable nor elastic but could provide services like gaming, videos, etc., to the user. The required storage and servers are used from public and local cloud providers.
4) *Local and Private cloud providers*—Having a limited scalability and elasticity was never been a problem for local and private cloud providers due to high performance, which provides efficient services to portable devices (considering delay, security, privacy, etc.).

The goal of Mobile Cloud Computing is to provide a better experience for mobile users whose devices have limited resources and capacities like computation, storage, battery [Rahimi et al., 2014]. Mobile devices do not need powerful configuration because all the complicated computing modules can be processed in the clouds, this describes Mobile Cloud Computing as a new paradigm for mobile applications [Dinh et al., 2011].

1.2.3. Mobile Cloud Computing Service Models

These services are used to construct architecture of MCC just like the service types which are used to build CC architecture [Chang et al., 2013]:

1) *Mobile Cloud Infrastructure-as-a-Service (MIaaS)*—This is pay-as-you-use model, where the client is provided with mobile cloud infrastructure and resources according to the value of his payment, where computing, storage resource, network components, and devices are provisioned, managed, and returned according to client's request in pay-as-you-use model.
2) *Mobile Network-as-a-Service (MNaaS*)—Vendor provides a diverse network infrastructure and resources to clients to respond to on-demand requests and dynamically configure, deploy, and design a wireless network infrastructure for the mobile connectivity, to the existing cloud infrastructure. The main advantage is the start-up cost is low due to high scalability and elasticity.
   e.g.: OpenStack, Google App Engine, MS Azure.
3) *Mobile Platform-as-a-Service (MPaaS)*—This service supports mobile application development, deployment, hosting, and validation tools.
   e.g.: App Mobi, is a tool which helps the user to develop, deploy and validate mobile application (as easy as possible).
4) *Mobile Software-as-a-Service (MSaaS)*—Here the clients are provided with mobility and location-aware capability software. In this model, mobile users are allowed to access mobile application services (which are deployed and executed on cloud) through thin mobile client based Internet communication.

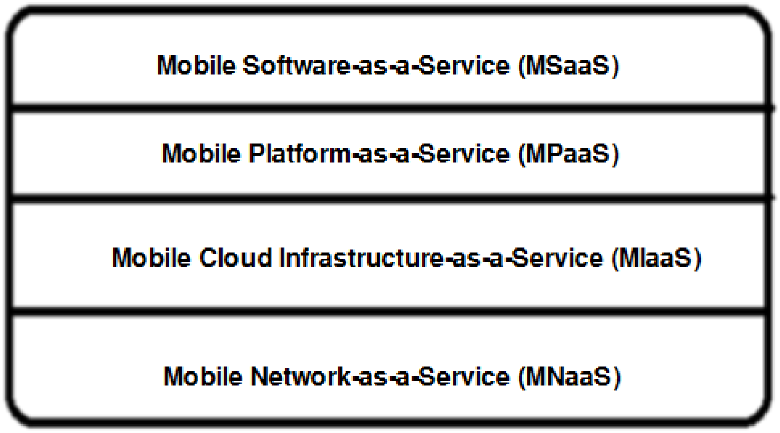

Mobile Software-as-a-Service (MSaaS)
Mobile Platform-as-a-Service (MPaaS)
Mobile Cloud Infrastructure-as-a-Service (MIaaS)
Mobile Network-as-a-Service (MNaaS)

Figure 6. Mobile Cloud Service Business Architecture (cf. [Chang et al., 2013]).

1.2.4. Advantages and Disadvantages of MCC

Advantages of MCC. Some of the advantages of Mobile Cloud Computing are [Dinh et al., 2011]:

1) *Extending Battery Lifetime*—Battery is one of the important components in a mobile device and its lifetime is the main concern to any mobile manufacturer. There have been many solutions proposed till date to reduce power consumptions like CPU performance, managing screen brightness etc. These changes are only possible with change in mobile infrastructure (hardware) but these changes might affect the cost of production and may not be feasible for all devices. To overcome all these challenges a technique, computational offloading was proposed, which helps the large and complex computations to migrate resource-limited devices (mobile devices) to cloud. This helps to cut down execution time of long/time-taking applications which results in energy consumption.
2) *Improving Storage Capacity*—Storage constraint is one of the most leading problems in today’s mobile devices. MCC this problem, which was haunting the mobile industry for past many years. Mobile users can now store/access any volume of data in the cloud without any storage restrictions. Some of the applications which use this cloud technique are Flicker [Flickr.com, 2017], Amazon Simple Storage Service [Amazon.com/s3, 2017], Facebook [Facebook.com], etc.
3) *Reliability*—Technology got revolutionized with the introduction of data backup and it even got better when reliability was introduced in mobile phones as data once deleted (even by mistake) could not be retrieved. MCC changed the way of storing data (by users). Now data can be stored in the cloud and can be used any number of times in any (different) device, this increases the reliability of the data.
4) *Dynamic Provisioning*—Waiting for a resource till the process complete its work has always been a problem in operating system, there are many resources scheduling algorithms which were used to allocate resources to the process according to the wait time. MCC solved this problem by introducing dynamic on-demand provisioning of resources which is a flexible way to run the applications without any reservations or wait time for the resources.
5) *Scalability*—Making changes or meeting user’s day to day demand takes a lot of effort and time for a service provider. This can be overcome by using flexible resource provisioning (provided by MCC), where the applications can be expanded (add/modify) with/without little constraint on the resource usage.
6) *Multitenancy*—This is the best way to reduce the cost of production (in software) as the resources are shared by large number of users (e.g.: network operator, data center owners, etc.).

7) *Ease of Integration*—Different user's request and demand can be handled by cloud service providers by integrating different services through the cloud and Internet without much effort (to meet the user demand).

Disadvantages of MCC. Some of the disadvantages of Mobile Cloud Computing are [Redekar et al., 2014]:

1) *Security*—Securing and protecting user information has always been a major concern. Mobile users store their important data in cloud, which must be protected else it can lead to major damage. So, protecting user information is one of the disadvantages in MCC.
2) *Performance*—Performance has always been a concern in mobile devices as its application feel is not as good as native applications. There would be some definite cut downs/changes in the mobile application when compared to actual application (which we use in our desktop).
   e.g.: Chase, this bank has its own mobile application for its users (to make transactions easy and fast). The application feel is different in mobile device when compared to PC/desktop, there are some cut downs like "Things you can do", this module is not available in mobile application (which cuts down the performance).
3) *Latency & Connectivity*—These things play a major role in data transfer. Even one poor connection/signal strength might cause delay in transfer of data. So, the service provider should regularly check bandwidth fluctuation and signal strength as these might get easily affected by weather, signal traffic, etc.
4) *Compatibility*—It is difficult for a mobile phone to switch between operating system as devices and applications are not homogenous. Different technology uses different application which makes it difficult for the service provider to work on consistent environment which decreases compatibility.
5) *Limited Resources*—Battery, memory storage, and other such factors have made the receiving and processing capabilities weak in mobile devices. This is because the processing power of a mobile device is less when compared to desktop/PC. Mobile devices have other limitation due to lack of resources which has become a hurdle in MCC.

1.3. Definition of Security and Privacy

Security—The right not to have one's activities adversely affected via tampering with one's objects [Al-Gburi et al., 2017].

In this section, we define our view of security services. The security services are shown in Figure 6, are as follows [Lilien et al., 2010]:

1) *Confidentiality*—The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

2) *Integrity*—The property that data has not been altered or destroyed in an unauthorized manner.

3) *Availability*—The property of being accessible and useable upon demand by an authorized entity.

4) *Authentication*—The corroboration that an entity is the one claimed, and the source of data received is as claimed.

5) *Access Control*—The prevention of unauthorized use of a resource

   a) Including the prevention of use [by authorized entity] of a resource in an unauthorized manner.

6) *Non-repudiation*—The prevention of entities' denial to be involved in all or part of a communication.

7) *Notarization*—The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time, and delivery.

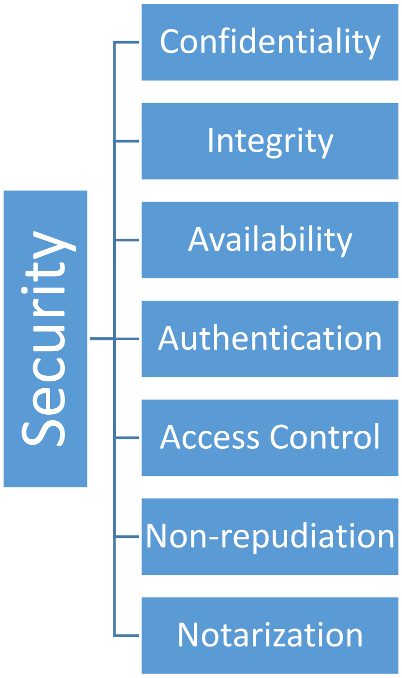


Figure 7. Security Services (cf. [Lilien et al., 2010]).

Privacy—The right to have information about oneself left alone [Al-Gburi et al., 2017]. Figure. 7, shows privacy services [Al-Hasnawi and Leszek Lilien, 2016]

1) *Confidentiality*—Protect information from unauthorized disclosure.

2) *Appropriateness*—Collecting, processing and retention of data has to be only as needed for legitimate purpose.

3) *Anonymity*—The state of being not identifiable with in a set of subjects called the anonymity set.
4) *Untraceability*—Making it difficult for the adversary to identify that a given set of actions were performed by the same subject.
5) *Unlinkability*—Hiding information about the relationships between any items.
6) *Unobservability*—Hiding items themselves.
7) *Notification*—Users have a right to be notified about the personal information collected by them and to give consent for its use.

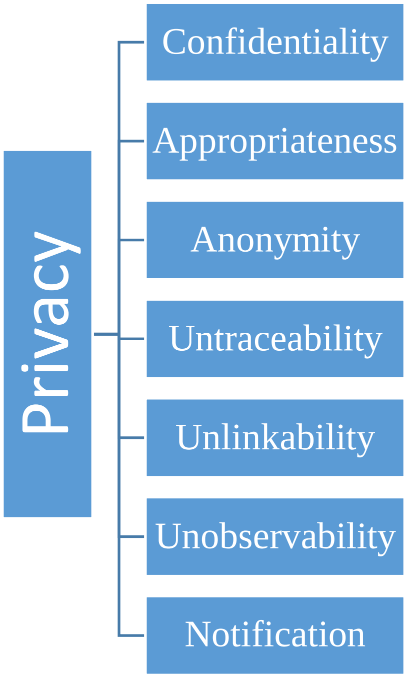


Figure 8. Privacy Services (cf. [Al-Hasnawi and Lilien, 2016]).

From Figures 6 and 7, it is obvious that confidentiality service is common to security and privacy services in other words, confidentiality represents intertwined of security and privacy.

Confidentiality. From the above statement we can say that, confidentiality is an intersection of security and privacy.

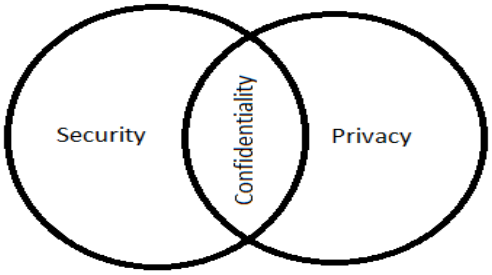


Figure 9. Intersection of Security and Privacy (cf. [Al-mawee, 2015]).

Security and Privacy in MCC are presented briefly in Sections 3 and 4, respectively.

1.4. Research Methodology

Research methodology is a logical and systematic search of new information on a topic which can be applied to a field of study [Rajasekar, 2013]. This may include publication research, interviews, surveys and other research techniques [Research Methodology, Businessdictionary, 2018].

In this survey, we have used forward and backward search (information together), where forward search identifies publications newer than the given publications. It is also a good way of searching for related information. Backward search identifies articles cited in a given publication, i.e., checking references in an article (the article is the one selected by the writer) [Padron, 2016]. Using these methods we have searched for the following papers: research papers, online sources, journals, magazines, etc., to gather information (to write the thesis). The above mentioned papers are searched on following websites: IEEE-Xplore, ACM digital library, Google Scholar, ResearchGate, Elsevier, Library loan, etc., to cover variety of MCC survey and other related topics.

During this search, we have used some keywords like “Mobile Cloud Computing”, “Security in MCC”, “Confidentiality of security and privacy”, “Components of MCC”, etc., in titles, abstracts or keywords of articles. Some of the references were excluded (after a careful review) because they are: (i) written in language other than English; (ii) duplicating knowledge from other papers; (iii) topics which are relevant but with less content; (iv) papers which talk about other things apart from the topic [Krishnan, 2017].

1.5. Survey Organization

This thesis is organized in the following way: (i) identifying what is MCC; (ii) how MCC works; and (iii) security and privacy of MCC.

Additionally, Section 1 presents overview of MCC; Section 2 covers MCC architectural approaches, which includes application (models); Section 3 discusses security in MCC; Section 4 discusses privacy in MCC; Section 5 discusses intertwined security and privacy in MCC and Section 6 concludes the Thesis.

2. ARCHITECTURAL APPROACHES TO MCC

This section starts with explaining the architecture of MCC then describes the middleware components of MCC. Later gives an overview of basic MCC services and ends with explaining application models for MCC.

2.1. Architecture of MCC

This section first present concept model to analyze MCC technology, then provides architectural scheme and ends with actual basic architecture of MCC.

Conceptual Architecture. Christensen proposed a three-component archetype model called Client-Connection-Cloud model [Christensen, 2009] for next generation mobile application which consists of three above three components: (i) client; (ii) connection; and (iii) cloud [Guan et al., 2011].

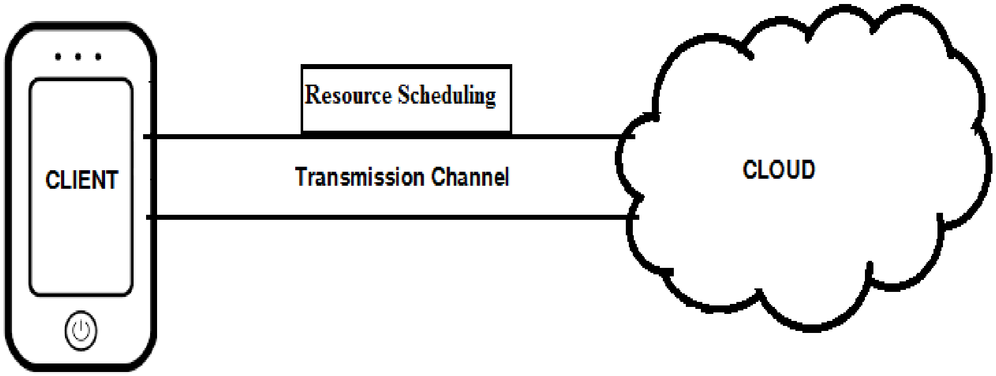


Figure 10. Basic Conceptual Model of MCC (cf. [Guan et al., 2011]).

Figure 8, shows us the conceptual architecture of MCC where the two entities client and cloud are connected through a transmission channel upon which are resource scheduling and content management, occupying client and cloud sides [Guan et al., 2011].

The transmission channel, resource and context scheduling are defined as follows:

1) *Transmission Channel*—It helps the data to transfer from one place to another with the help of wireless transport protocols. In MCC the connection between client and cloud is like a double edge sword where one weak transmission degrades the performance and the other increases prosperity of mobile application (due to dynamic character of connection).
2) *Resource Scheduling*—Scheduling of resources (computing, storage, etc.) using virtual machines are addressed in MCC. In MCC, we try to disintegrate complex applications to

simple (and small) application which are handled parallely (but each application is given individual care).

Architectural Scheme. This is an organization of MCC system, where researches either try to improve mobile device capabilities using cloud technology or use cloud technology on behalf of mobile device to execute mobile applications. This architecture has two schemes [Guan et al., 2011]:

1) *Agent-Client Scheme*—Cloud provides resources to mobile devices, this overcomes the limitations of mobile device like power, storage, etc. Figure 9, illustrates an agent-client relationship where the cloud provides agent to each individual client (mobile device). Each client communicates with cloud or other clients (outside its domain) using the agents (provided by the cloud).

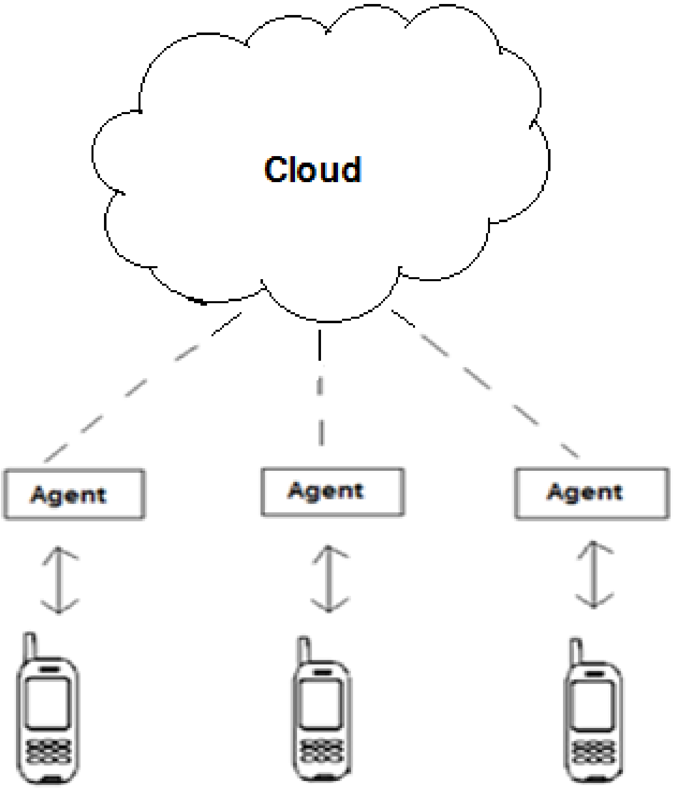


Figure 11. Basic Agent-Client Scheme (cf. [Guan et al., 2011]).

Mahadev Stayanarayanan proposed model which stands as an example for agent-client scheme, called cloudlet architecture [Satyanarayanan et al., 2009]. Before introducing cloudlet architecture, let us discuss few things about non-cloudlet architecture, which paved a way for introducing cloudlet architecture.

a) *Non-Cloudlet Architecture*—There are three components in this architecture they are mobile client, transmission channel and Cloud as shown in Figure 10. Mobile client requests services from cloud, cloud provides the requested services (where the cloud is owned by an organization or cloud provider) to the client this is done using transmission channel. Though there is a good relationship between client and cloud there is a drawback in this architecture, communication latency. To overcome the latency problem cloudlet architecture came as a solution [Malik et al., 2013].

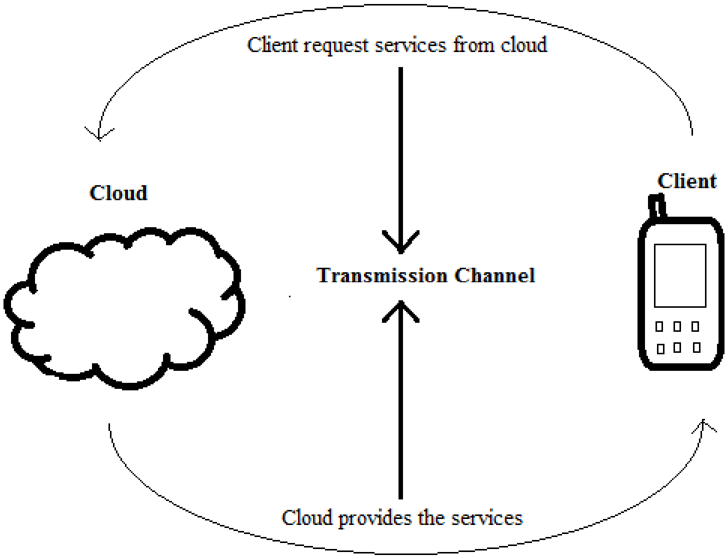

Client request services from cloud
Cloud
Client
Transmission Channel
Cloud provides the services

Figure 12. Non-Cloudlet Architecture (cf. [Fernando et al., 2013]).

b) *Cloudlet Architecture*—Figure 11, shows the cloudlet architecture (owned by local business) which is installed between client and cloud, which contains cached copy of data. The cost is less when compared to cloud as each cloudlet has only one data center with few users' due to which it has less communication latency when compared to non-cloudlet architecture [Malik et al., 2011]. Mahadev Satyanarayanan proposed a cloudlet architecture based on Guan architecture, where a service is customized on a virtual machine by mobile user on nearby cloudlet, which is later used over wireless LAN.

This implementation helps associated mobile devices to use memory, processing, and storage using Wi-Fi access points (extended from natural implementation) [Guan et al., 2011].

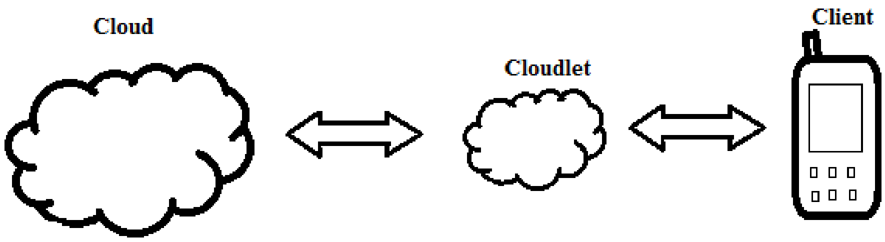


Figure 13. Cloudlet Architecture (cf. [Fernando et al., 2013]).

The other scheme in architectural scheme is:

2) *Collaborated Scheme*—In this scheme, cloud is used inside a mobile device, which helps the cloud to use remaining resources of mobile device. Here cloud acts as controller and scheduler. The below figure illustrates collaboration among mobile devices where each device interacts with other devices using its cloud (outside its domain as well) [Guan et al., 2011].

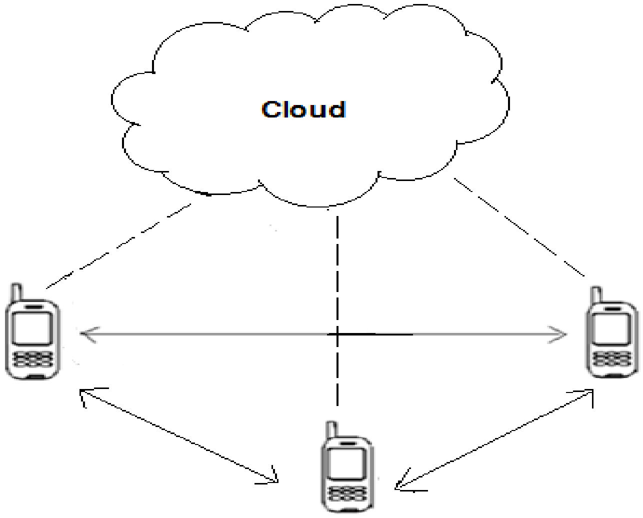


Figure 14. Collaborated Scheme (cf. [Guan et al., 2011]).

Basic Architecture. This a generic architecture of MCC consists of two different mobile networks A and B as shown in Figure 13 [Shahzad et al., 2014], where all the mobile devices are connected to their respective network (mobile) via base stations like BTS (Base Transceiver Station), AP (Access Point), and satellite. These base stations play a major role in establishing and controlling connections and functional interfaces between mobile devices and their respective networks. When a request/information is requested by the user, it gets transmitted to central processors. These processors are connected to servers which consists of database, hashing algorithm, and AAA (Authentication, Authorization, Accounting) framework which provides mobile network services. Once the request gets transmitted, it leaves the mobile network and connects with the cloud through Internet. Inside the Cloud Computing, cloud controllers link the user's request with the relevant cloud depending upon the requested service. Once the requested information is processed, the cloud sends back the service to the central processor.

Upon receiving the request, the central processor with the help of mobile network operator provides the requested information to the user according to the user level (stored in the database). This is done with the help of AAA framework, to keep a track of user and to know who is trying to access/request sensitive information. Those requests which are provided to the users upon their requests are nothing but their corresponding cloud services [Dinh et al., 2011].

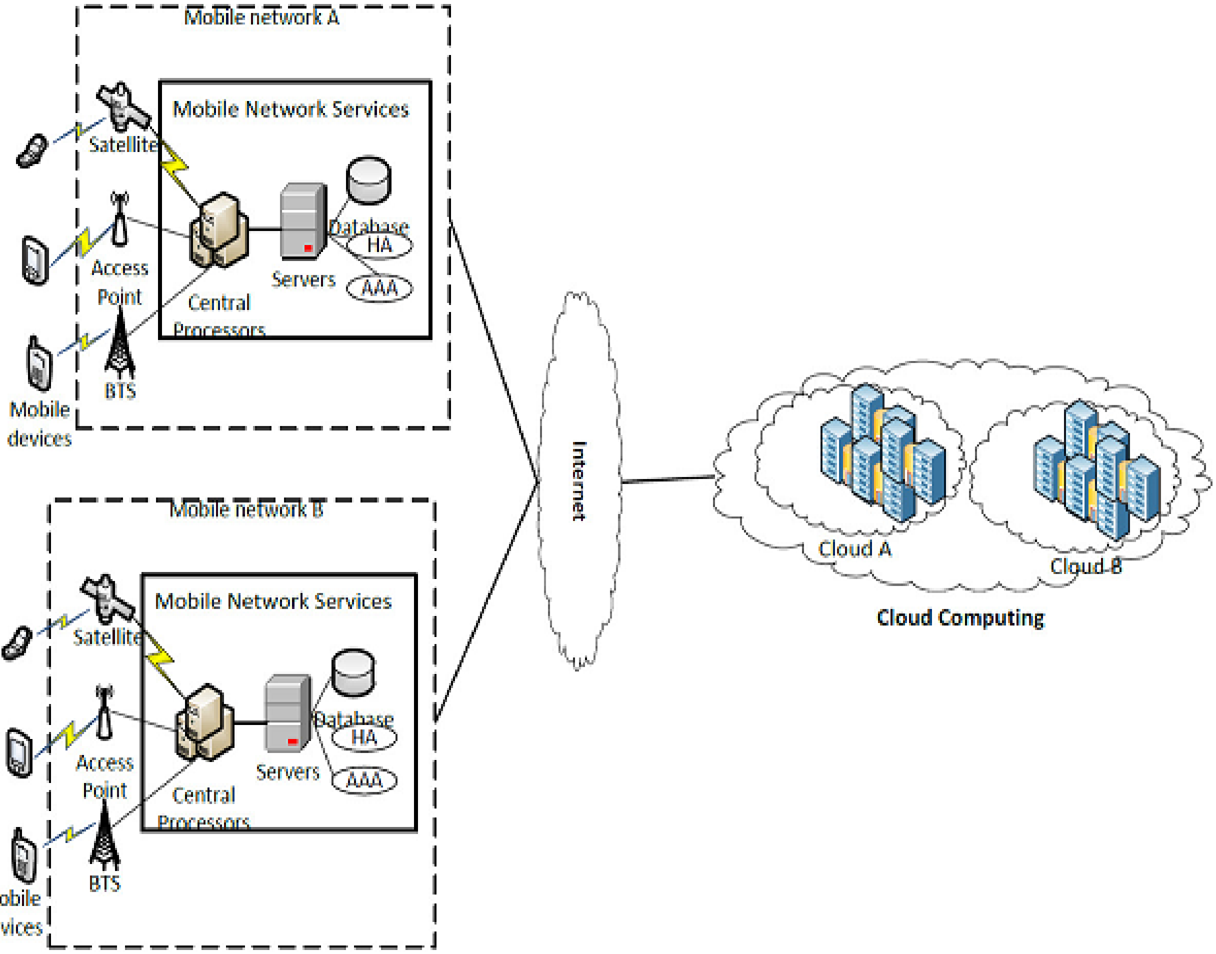


Figure 15. MCC Architecture (cf. [Mobile Cloud Computing, Wikipedia, 2017]).

2.2. Middleware Components for MCC

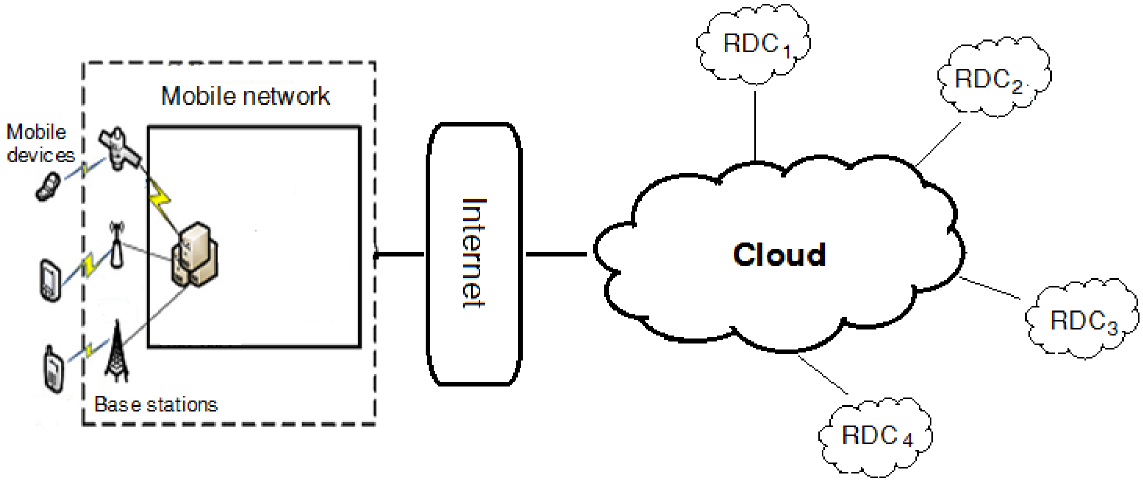


Figure 16. Components of Mobile Cloud Architecture (cf. [Bahl et al., 2012])

The components are:

1) *BS*—Base Station, a transceiver that connects a cordless phone or wireless device to a central hub and allows connections to a network [Base Station, Wikipedia, 2017].
2) *RDC*—Regional Data Centers, is a facility used to house regional computer systems and associated components such as telecommunication and storage systems [Regional Data Center, Wikipedia, 2017].
3) *Storage Node*—A storage node is typically a physical server with one or more hard disk drives (HDDs) or solid-state drive (SDDs) [Rouse, 2017a].
4) *Compute Node*—A compute node provides the ephemeral storage, networking, memory and processing resources that can be consumed by virtual machine instances [Compute node, Wikipedia, 2017].

The above figure illustrates how the middleware components of MCC works, to help the user store the data in the cloud or request the stored data in the cloud.

Users' request is transmitted to the central processor (in mobile network) via base stations. The request is transmitted to the cloud via Internet. Once the requested is received, the cloud controller (in the cloud) links the request to respected RDC (depending upon the user request and location), where RDC's can store and manage the data, exchange data, access data, etc. Once the request is received, RDC processes the request and sends back the requested information to the cloud. Cloud sends the request back to the central processor via Internet. Central processor sends the data to the user via base station.

2.3. Basic MCC Services

Cloud computing providers provide a set of basic services for mobile computing. There are three types of services they are application services, platform services and context rich services [Bahl et al., 2012]:

1) *Platform Services*—The services (EC2) which are accessible from mobile devices are called platform services like database, storage, etc. Application sharing helps some of these services (by benefiting them). For example, memcache helps applications to create or access same data sets, this will reduce the computation demand of re-generating cached results. These services also help to create new services like file backup, file syncing using storage and computing services.
2) *Application Services*—Some of the application services are offered by public cloud provides, they are:
   a) *Location-Based Services*— Presence service can be one of the essential service in location based services. People usually do not trust these services due to privacy issues. So, the best possible solution for this would be using cloud services. These services provide privacy from unauthorized user using presence service, where the presence service implements location privacy policies specified by mobile users (as different users have different level of privacy requirements). This would gain the trust of the people, which will increase the development of location based services.
   b) *Video-Streaming Application*—Mobile devices have problems in video streaming due to limited bandwidth and video codec. The cloud provider eliminates this problem by offering video transcoding and streaming proxy, where the proxy service reduces the bandwidth and codec problem by performing transcoding (in the cloud).
3) *Context Rich Services*—Recognizing location of the user, the time of day, user’s identity and their personal preferences make mobile applications more context aware. There are three context rich services, they are:
   a) *Context-Extraction Service*—In a mobile device there are different types of data, social networking data, sensor network data, etc., these data are mined (using data mining analysis) to extract clues related to the user. Apart from this, context extraction service also reduces duplication of data, which saves energy and decreases computation cost of the mobile device.
   b) *Recommendation Service*—It creates output based on contextual clues, which fits an individual or a set of individuals. In cloud, the output would be multimedia output for mobile devices or nearby multimedia device.
   c) *Privacy Service*—New privacy services needs to be created in context rich services. For example, location services need new privacy services that are created to protect user data from data mining. Similarly, data released from social networks and sensor networks need new privacy services. Sometime in near future group services will also

emerge that protects the group of individuals from their actions, taste, and preference inference.

2.4. Application Models for MCC

Some parameters play an important role in the acceptance of any mobile cloud application model, the model which address most of the following parameters are considered to be preeminent. The following parameters are used to compare the application models [Khan et al., 2014b]:

1) Context Awareness
2) Latency
3) Bandwidth Utilization
4) Generality
5) Privacy
6) Complexity
7) Security
8) Programming
9) Scalability
10) Execution Resource
11) Platform

The mobile cloud application models are designed to achieve objectives such as to enhance performance of an application, to achieve energy efficiency, etc. Sometimes these objectives may conflict with each other so, these models should be considered based on the objectives and conflicts. There are four categories of mobile cloud application models (based on thhe above objectives), they are:

1) *Performance-Improving Application Models*—These models increase the performance of mobile device application by offloading complicated computations to the cloud (where the computations are executed in less time when compared to mobile devices). There are two types of performance based application model:
    a) *Clone Cloud Model*—This model offloads some parts of complicated application to the nearby infrastructure or cloud to increase the performance.
    b) *Zhang et al*., *Model*—This model uses weblets, an independent functional unit of an application. The weblets offloads the computation based on mobile device battery, memory, etc. If the computation is complicated (cannot be computed in mobile device), weblets offloads the computation to the cloud. This model is based on elastic application technique.
2) *Energy-Improving Application Model*—They reduce energy consumption in mobile devices. It can be done by performing intensive computations in the cloud. This helps the mobile applications to consume less energy. Cloud is one of the energy based application models.

    a) *Cloud Model*—In this model, applications are organized using heterogeneous components. To achieve such organized applications graph are used, where each component either executes in mobile devices or cloud or both. This way it helps the mobile device to consume less energy.

3) *Constraint-Overcoming Application Models*—In these model's regular components are executed in mobile devices and complicated components are executed in the cloud (where the local resources are insufficient). There are three types of constraint based application models:
    a) *Satyanarayanan et al., Model*—This model uses virtual machine concept, where a computer or a set of computers are called cloudlet. The intensive components are offloaded to cloudlet for execution by the mobile device (which acts as thin client).
    b) *Giurgiu et al., Model*—This model partially offloads intensive components to the cloud. It is based on distributed layers technique.
    c) *Extensible Cloud Model*—It uses stack on demand technique on top of VM systems, where the top stack frames or segments of the frames are offloaded to the cloud.
4) *Multi-objective Application Models*— These models are mainly used to achieve multiple objective at the same time. This is more effective than the other application models. There are three types of multi-objective application models:
    a) *MAUI*—It mainly focuses on minimizing energy consumption. MAUI does it by offloading intensive application to nearby infrastructure or cloud (only when it thinks that the offloading woukd minimizes energy consumption).
    b) *ThinkAir*—It is designed to achieve Quality of service (QoS). The resource intensive methods are offloaded to the cloud (the programmer identifies all intensive methods for remote executive).
    c) *Cuckoo*—It is designed to make the programming easy (for the developers). The applications are partially offloaded to nearby infrastructure or cloud.

Application Model Comparison and Examples. The following are the application model comparison and examples:

1) *Model Comparison*—Table 1 represents comparison models as given in ref. [Khan et al., 2014b].

Table.1 Comparison of the Application Models [Khan et al., 2014b]

	Model	Ca	La	BU	Ge	Pr	Co	Se	Pa	Sc	Er	Pt
Performance Based Application Model	Clone Cloud	Med	Low/ High/ Med	High	Med	Low	High	Low	High	Low	NI/CL	Android
	Zhang *et al*., Model	Med	Med	Low	High	Med	Low	High	High	High	CL	.Net(C)
Energy Based Application Model	µCloud	Low	Low	Low	Low	Low	High	Low	High	Low	CL	Android
Constraint Based Application Model	Satyanarayana *et al.,* Model	Low	High	Med/ High	Low	Low	Med	Low	Med	Low	NI	Virtual Box
	Giurgiu *et al.*	Low	Low	Low	Med	Med	Med	Low	High	Med	NI	Java
	Extensible cloud	Low	Med/ High	Med	Med	Med	High	Low	High	High	NI/CL	iOS
Multi-objective Based Application Model	MAUI	High	Low	Low	High	Low	Low	Low	High	Low	NI/CL	Microsoft .Net
	ThinkAir	High	Low	Low	High	Low	High	Low	Low	Med	CL	Java
	Cuckoo	Low	Med	Low	High	Low	Med	Low	Low	High	NI/CL	Android

Ca: Context Awareness
La: Latency
Bu: Bandwidth Utilization
Ge: Generality
Pr: Privacy
Co: Complexity
Se: Security

Pa: Programming Abstraction
Sc: Scalability
Er: Execution Resource
Pt: Platform

CL: Cloud
NI: Nearby Infrastructure
H: High, M: Medium, L: Low

2) *MCC Application Examples*—Here are few more examples of MCC applications to show how this technology can prove beneficial for various domains [Khan et al., 2014b], they are:

    a) *Mathematical Tools*—Mobile devices can offload complex mathematical calculation such as a large matrix to the cloud. This increases the performance, efficiency and decrease large amount of energy used. This type of application can be developed using MAUI, Think Air.

    b) *File Search*—Searching a file, which is stored in a large storage usually takes a minute or two. MCC enhances the performance, which makes it easy to search a file (within fraction of time)

    c) *Download Applications*—To download a large file, mobile device (with low data rate) consumes a lot of battery power, storage, and time. MCC makes it easy, it allows users to download files in the cloud and transfer files to mobile device. This technique enhances battery power, reduces time, efficiently stores the file (according to the size), and downloads the file to mobile device in high speed.

    d) *Antivirus Applications*—To safe guard important/sensitive information, user's need to install antivirus in their mobile device(s). Scanning a device consumes a lot of energy and processor time. This issue can be resolved using MCC, which clones the mobile device and scans the clone for malware in the cloud. This saves both energy and time.

    e) *Security*—User's install large number of applications in which some of them might be unsafe. Such applications might attract attackers, which can jeopardize sensitive information stored on smartphones. MCC is used to overcome this problem, it allows mobile devices to execute their services in the cloud. This increases the security for user's sensitive data stored in the device.

    There can be hundreds of similar applications that can take advantage of MCC. However, the objective of using MCC must be known before adopting any application model. The application models must be chosen wisely to achieve the desired objective(s).

2.4.1. Challenges in Building MCC

The following are the challenges in building MCC application [Wang et al., 2014c], they are

1) *Code/Computation Offloading*—Application performance and conservation of mobile device energy can be enhanced (while building MCC applications) but code/computation offloading might cause an issue during this process. There are two process, which helps in overcoming this design issue, they are:

   a) *Application Partitioning*—In this process an application is partitioned into small pieces so that they can be easily processed in the cloud. Code offloading makes use of this method, where the application is divided into exact small pieces (in an efficient manner) with proper pause, if the break point (pause) is not set properly, it can degrade the performance of the applications. This process also requires a cost model to cut down the overall cost (accordingly).
   e.g.: Partitioning of applications using threads and clone cloud [Chun et al., 2011]. Both the methods try to divide the application in an efficient manner such that the performance would increase and the cost would decrease accordingly.

   b) *Making Smartphones Last Longer with Code Offload (MAUI)* [Cuervo et al., 2010]—It helps code offloading by providing an architecture which points out problems like energy and performance issues. MAUI helps the client and server to build their own proxies, profilers and solvers instead of cloning the services from client to server. Here the developers need to recognize the methods/classes (manually) which are capable of getting executed remotely. The developers cannot select API code, etc., (for offloading) due to constraint issue. Later, the system has to dynamically determine whether or not the offloading is beneficial (this is done during processing) and lastly, the client needs to be connected with the server and if the developer fails in connecting it, the proxy will reinvoke the method locally or run it on other servers.
   e.g.: Cuckoo [Kemp et al., 2012], ThinkAir [Kosta et al., 2012].

2) *Elasticity and Scalability*—This is the third design issue, the application should be scalable and elastic, where scalability [Scalability, Google search, 2017] is the capacity to be changed in size and this relies on allocating resources (to VM) and elasticity [Elasticity, Google search, 2017] is the capability of resource, where the resource have no limits and can be used in any quantity. There are many papers on this issue and there have been some solutions suggested to make an application both elastic and scalable like resource allocation, some algorithms, etc., but these are all just suggestions, there are still some research going on how to overcome these issues.

3) *Security*—Users can be convinced to use MCC applications after dealing with certain security issues. On the cloud side, the application must make sure that the resource is accessed by an authorized user. On the user side, the application must make sure that there is authentication, authorization, and data or code integrity, let us see how:

   a) *Authentication*—It is one of the security issue. As authentication is bi-directional, it uses mobile-cloud authentication where the client authenticates the cloud and client-cloud authentication where the cloud authenticates back to the client. The research shows that all the work cited are on mobile-cloud authentication like web authentication [Bonneau et al., 2010], mobile to cloud authentication framework [Al-Muhtadi et al., 2002], Kerberos based mobile to cloud authentication [Harbitter andMenasce, 2011]. The cloud-client authentication needs more work and there are some research work going on in this topic. One such topic is message digest based authentication for MCC, where it concentrates on both client-cloud and cloud-client authentication.

b) *Authorization*—This is another issue for MCC applications. Users are authorized to access their data without credentials (all the time), which might save energy of the device but accessing information without authorizing it may create a lot of problems. Example: Google, Twitter, Snapchat, and Facebook, use OAuth 2.0, a single sign on application.

c) *Data/Code Integrity*—Encrypting data and storing it in a remote server is not at all a problem in PC/desktop but when coming a mobile device, it is difficult to encrypt a data due to computational cost and it does not work practically. To overcome this issue Van Dijk et al., developed a protocol, which allows the user to encrypt and store the data in the cloud. This protocol helps in reducing the cost and maintaining the security the data by storing the encryption key and the data in the cloud.

4) *Cloud Pricing*—The user can request more resources by paying more. This might affect cloud service disciplines and admission policies. Some of the cloud pricing strategies are proposed to increase service provider's profit and/or to reduce user's cost:

   a) Dynamic Virtual Machine Provisioning [Zaman et al., 2013].

   b) Cloud Capacity Segmentation [Wang et al., 2012b].

   c) Virtual Machine Spot Binding Policy [Zafer et al., 2.012]

   d) Linear Programming [Lampe et al., 2012].

   e) Pricing Mechanism [Li et al., 2011].

The works cited above are just theoretical but has no real traces, research work is going on in this topic which might help us to pave a way to solve some issues.

Each challenge, existing solutions and future research directions (for building MCC application) are discussed in tabular form.

Table 2. MCC Application Challenges, Existing Solutions, and Future Research Areas (cf. [Shahzad et al., 2014]).

Challenges	Related Issues for Challenges	Suggested Solutions	Possible Future Solutions (for the challenges)
Code/Computation Offloading	No related issues	Application partitioning MAUI	Automation of code/ computation offloading.
Elasticity and Scalability	No related issues	No exact solution is suggested yet, research is still going on.	Research is still going on.
Security	Authentication	Mobile to Cloud, Cloud to Mobile	Cloud to mobile authentication.
	Authorization	OAuth 2.0	Authorizing without releasing user credentials.
	Data/code integrity	Encrypting data	Research is still going on.
Cloud Service Pricing	No related issues	Dynamic virtual machine provisioning. Cloud capacity segmentation. Vitual machine spot binding policy. Linear Programming. Pricing Mechanism.	Research is still going on.

3. SECURITY AND PRIVACY IN MCC

This section first presents security problems in MCC, which includes security threats and solutions. It also provides solutions for related problems.

3.1. Security Problems in MCC

Security and privacy are never ending issues in MCC. These issues are inherited from various domains from which Mobile Cloud Computing is derived. Mobile Cloud Computing is derived from Cloud Computing, Mobile Computing, and Wireless Networks so, the security issues of Mobile Cloud Computing inherits the security issues of Cloud Computing, Mobile Computing, and Wireless Networks [Malik et al., 2013]. The following are the security issues in mobile cloud computing [Suo et al., 2013]:

1) *Mobile Terminal*—Mobile Terminal has some characteristics which might cause some serious issues:

    a) *Malware*—It is a process of damaging or disabling information in mobile devices. Openness and versatility in any device always draw attacker's attention. An attacker always looks for vulnerable devices, after finding a device he tries to attach the malware (virus, worm, etc.) to a program (even useful software's) which the user might download unknowingly. The downloaded malware crashes the security system of the mobile device and waits for the attacker's command. Later, with the help of malware the attacker gets hold on all important information stored in the device and can try to misuse it. For example, the attacker can do automatic payment without user's involvement. This would lead the user to suffer from information leakage. Even though there are anti-virus software's for mobile phone, it does not provide functionality similar to desktop due to capacity and resource constraints, which makes it difficult for the software to achieve significant computation.

    b) *Software Vulnerabilities*—A software can become vulnerable due to many factors but some of the important one's are application, operating system, etc.

        Vulnerabilities in application software's are common, due to which they are not rigorous. This nature attracts the attackers to attack the device using malicious content.
        e.g.: if a bank's application software is vulnerable (no strong security and privacy technique), it indirectly opens a gate for the attacker, who tries to hack the system. Later, he tries to access user's sensitive information (SSN, user's account details, etc.), due to which the user suffers (ultimately).

        Apart from applications, OS can also be vulnerable. An attacker takes advantage of the vulnerability in OS and attacks the device. Sometimes the mobile users themselves create some issues like downloading files, clicking unsafe links, etc.

These things also help the intruder to attack/hack the device (mobile). So, the users and the developers need to be aware of such attacks, to prevent them.

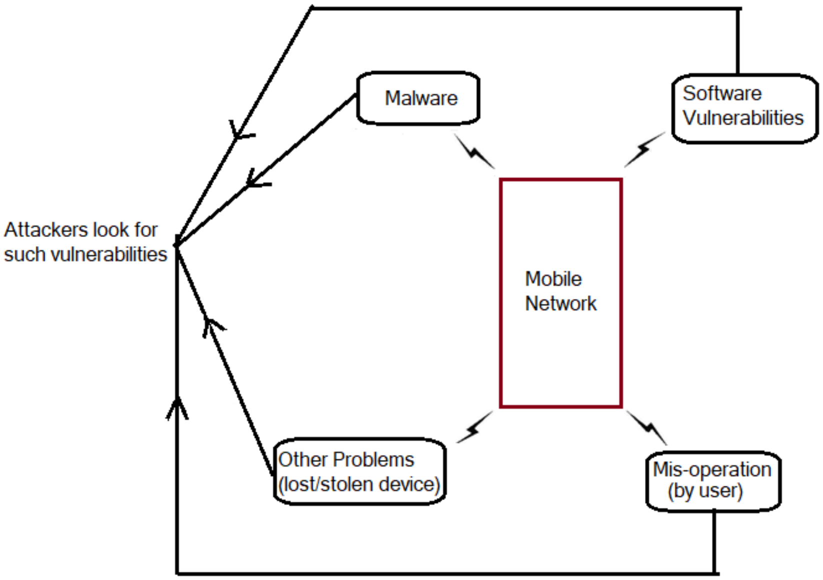

Malware
Software Vulnerabilities
Attackers look for such vulnerabilities
Mobile Network
Other Problems (lost/stolen device)
Mis-operation (by user)

Figure 17. Mobile Terminal Security Threats (cf. [Suo et al., 2013]).

2) *Mobile Network Security*— Broad access like 3G, Wi-Fi, etc., brings in more security threats such as information leakage or attack.
e.g.: Today's restaurants provide free Wi-Fi to their customer's. Due to weak Wi-Fi encryption, the attacker's try to attack the network which may lead to information leakage. In some cases, the attacker's may even try to attack a private network like 3G. In this case, the attacker usually targets 3G or Wi-Fi networks with weak encryption, which may lead to data loss.
Sometimes the user's themselves can mis-operate things, this may lead to security issues. Awareness needs to be developed among the users to prevent such things from happening.

3) *Mobile Cloud*—

   a) *Platform Reliability*—Any one like an employee of a company, a malicious attacker, etc., might try to steal information from the cloud as it is a high concentrated source of user's information. The person/attacker tries to steal the information to shut down the cloud service. The user's and the cloud providers should be made aware of such attacks. The cloud providers should integrate newer version of security technologies, while the user's need to back up their data instead of depending completely on the cloud provider.

   b) *Data and Privacy Protection*—Data ownership and management of the user's data is handled by different people; the ownership is with the user but it is managed by the cloud provider. This might cause some users to think about their data storage in MCC, which might affect MCC popularity. The other issue is that, the user's data is stored in shared infrastructure in an unknown location (which can be anywhere in the world) and the cloud providers do not enclose the location of the user's data to the user. These two issues increase the risk of exposure (user's data). So, to protect the sensitive data there need to be a permanent solution which helps to protect user's data security and privacy.

These are some of the other security problems suggested by [Mollah et al., 2017]. MCC utilizes many traditional as well as recent technologies such as offloading, virtualization, outsourced storage, etc., and it adopts several new security problems along with traditional problems. This section, presents the list of potential security problems within MCC:

1) *Data Security Problems*—Cloud stores and process user's data (at service provider end) which invites some security problems like data loss, data breach, data recovery, data locality, etc.:
    a) *Data Loss*—Data can be damaged by any physical means during processing, transmission and storage.
    b) *Data Breach*—Data can be copied, stolen and used by unauthorized person.
    c) *Data Recovery*—The process of recovering data from damaged, corrupted, stolen or lost data (in mobile device).
    d) *Data Locality*—User's need to know the location of their data. Data of each individual needs to be stored separately else the data can become vulnerable.
2) *Offloading Security Problems*—Mobile users do not have control over offloading process and to offload their data with control, they need to access cloud during the process. This makes it easy for any unauthorized user to access the offloaded data. Another issue of offloading process is, executions are done at the cloud side (instead of mobile devices), which might possibly violate the integrity and confidentiality of the offloaded content; where integrity is violated due to after execution of offloaded content and confidentiality is affected due to the presence of malicious content between partitioning and offloading stage. As the executions are done at cloud side, mobile devices cannot verify the result of these executions, even if they are not correct or altered.
3) *Virtualization Security Problems*—Virtualization refers to act of creating a virtual version of something. Virtualization technique helps the user to use cloud services (provided by cloud service provider). Virtualization clone's mobile devices in the cloud end using virtual machine (for processing). This process when applied to MCC, generates several security problems like unauthorized access, VM to VM attack, etc.
4) *Mobile Cloud Applications Security Problems*—These level of attacks can affect integrity and confidentiality of the data and application. The attacker tries to inject one of the malware's (virus, Trojan etc.) into the target application which changes the functionalities of the application.
5) *Mobile Device Security Problems*—The most common threat is misplacing/losing a mobile phone which can disclose important information to an unauthorized user. The data stored in the cloud can also be disclosed by the attacker by accessing cloud services from the mobile device using some tools or techniques. Although there are some security features to keep the phone unlocked (which can prevent the attacker from accessing the data), the

attacker can still unlock it by removing the original identity module card and reinserting virus infected identity module card, which might unlock the phone. Even though the platforms of mobile devices are almost equal to that of a PC/desktop, they still lack in security mechanisms and this problem affects the integrity of the mobile device (application).

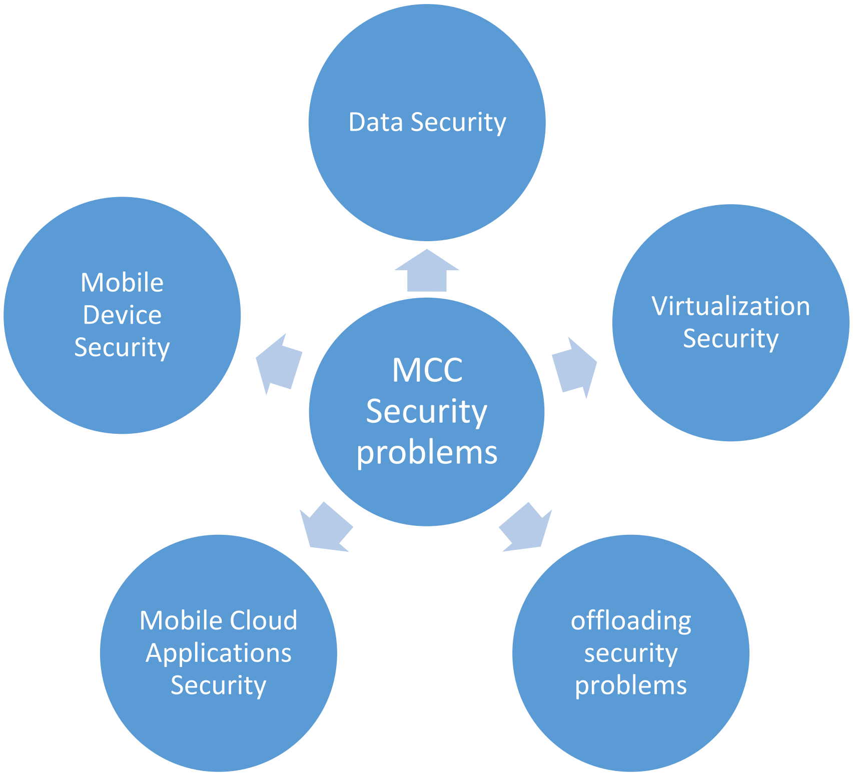


Figure 18. Security Problems in MCC (cf. [Mollah et al., 2017]).

3.1.1. Security Threats

These threats are also divided into four categories [Vikas S. et al., 2014]:

1) Physical Threats
2) Network-Based Threats
3) Web-Based Threats
4) Application-Based Threats

1) *Physical Threats*—Mobile devices has become a part of our lives, where we use it for personal and professional things. Mobile devices contain regular as well as sensitive information which can be easily hacked so, physical security for a mobile device is very important. There are some ways to explain physical threats:

   a) *Company Device*—These days almost every company provide its employee with mobile devices, laptops, etc., to maintain the privacy. If an employee misuses the privilege by using it for personal use (just to cut down their cellphone costs), there is a risk of data loss. Let us take a scenario, an employee (carrying his business phone) goes to a coffee shop, while leaving, he forgets his device, the attacker who is stalking him steals the device, unlocks it (using some tools or technique) and tries to retrieve all the sensitive information (like his company's email id, which provides access to all intranets and portals and provides the login key to nearly all enterprise designed productivity and collaboration tools), which might land the employee into big trouble.

   b) *Lost or Stolen Devices*—This is one of the most common threats. Losing a mobile device might land the owner into a lot of problems (as specified in the above scenario).

2) *Network-Based Threats*—Wireless network can be a host to all sort of threats, like:

   a) *Unsafe Network(s)*—If a user connects to an unknown network like Wi-Fi at airports, coffee shops, etc., then there is a chance that the attacker might install the malware into the user's device without their knowledge.

   b) *Wi-Fi Sniffing*—It is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans. This is created for capturing data on wireless networks. Hackers can use this software to steal user's data, spy on network activity, logins, etc.

   c) *Denial of Service*— It is a process where the intruder makes a network or a resource unavailable to the user by disrupting host services. The intruder accomplishes this by flooding target machine or resource with redundant requests in order to overload the systems, which prevents legitimate requests from being fulfilled. There is another attack similar to DoS called, Distributed Denial of Service (DDoS), where the attacker tries to flood the user's system using different system's sources, which makes it almost impossible for the user to stop it (as the user tries to stop it (only) from single source).

   d) *Session Hijacking*—Misusing a valid session key to gain unauthorized access to information or services in a computer.

e.g.: In a session, node A sends a packet to node B, after verification (from node A), node B sends reply to node A. In-between the attacker tries to attack the session using session key, he does it by attacking either one of the node's (A or B). Later he tricks both the nodes to grab all the important information.

3) *Web-Based Threats*

   a) *Phishing*—These are fraudulent messages appearing to come from legitimate company. These messages usually direct the user to a spoofed website or ask the user to provide secured information like credit card information, bank details, etc. This information is later used by the attacker to commit identity theft.

   b) *Drive-by Downloads*—Here there would be either an authorized download without understanding the consequences or content getting downloaded without user's knowledge. In both the cases the user would be the ultimate person to suffer [Drive-by download, Wikipedia, 2016].

   c) *Browser Exploits*—It is a form of malicious code which tries to breach browser security by taking advantage of flaw or vulnerability in an O.S. or part of software to alter user's browser settings without their knowledge.

4) *Application-Based Threats*

   a) *Malware*—"It is a software which damages/disable software in user's system or performs malicious actions without user's knowledge." [Malware, Wikipedia, 2017].
   e.g.: An attacker sends a malicious software into a user's mobile device, it makes its way into the system, later upon attacker's command the software might send undesired messages to the people in user's contacts list, or it can retrieve user's personal data, which can be misused by the attacker.

   b) *Spyware*—"[It] gathers information about a person or organization without their knowledge, that may send such information to another entity with consumer's consent, or that asserts control over a device without consumer's knowledge. It is mostly used for the purpose of tracking and storing Internet user's movements on the web," e.g.: Internet Optimizer is one of the spyware attacks, where it hijacks error pages and redirects them to its own controlling server. When users follow a broken link or enter an erroneous URL, they see a page of advertisements. However, because password-protected Web sites (HTTP Basic authentication) use the same mechanism as HTTP errors, Internet Optimizer makes it impossible for the user to access password-protected sites. Later it downloads and runs itself on the user computer without their permission [Spyware, Wikipedia, 2016; Spyware, FTC, 2016].

   c) *Vulnerable Applications*—Even a small flaw in an application might lead to the whole software getting hacked. Such vulnerabilities give the ability to the attacker to hack sensitive data, stop a service from functioning, etc., even a small bug might cause problems to the system. Regularly fixing and maintaining the systems helps preventing such things.

d) *Unlicensed and unmanaged applications*—Unauthorized applications can price a company in legal costs but whether or not applications are licensed, it needs to get updated regularly to repair vulnerabilities that might be used to attain unauthorized access/steal information.

3.2. Security Solutions in MCC

Some of the security solutions for the problems suggested by [Mollah et al., 2017] are:

Data Security Solutions. Data always invites security problems, some of them are specified in section 3.1 (in Data Security), now let us see how to securely store data to avoid problems:

1) *Distributed Multi-cloud Storage, Data Encryption and Data Compression*—The data is divided into segments, where each segment is encrypted and stored on multi-cloud storage. Even if an attacker tries to compromise one of the cloud storages, the other cloud storages would be safe (as the data is divided and stores on mutli-cloud) [Alqahtani et al., 2014].
2) *Secure Sharing, Scalable Watermarking, and Reed-Solemon Coding*—This technique consist of three parts: (i) Secure sharing, is used to upload multi-media data (in different segments) to multi-cloud storage(s); (ii) All these storages are authenticated using watermarking method, which authenticates data at content level. This method can be scaled up and down according to network bandwidth, battery, and display conditions (as it is scalable; (iii) Reed-solemon coding ensures safe transmission of data even in error-prone wireless network [Wang et al., 2014a].
3) *Block-based Sharing Scheme (BSS)*—It is a cryptographic method, which logically divides the data into blocks. Each block is encrypted and decrypted to reconstruct the data into its original form. This method not only provides better security by reducing the computations of intense security operations but also concentrates (mainly) on confidentiality and integrity of the data. This method is constructed based on another method called, remote data auditing [Khan et al., 2014a].
4) *Public Auditing Protocol*—It uses asymmetric group key and proxy re-signatures: (i) asymmetric group key, allows public and private key sharing among group members and create tags (for files); (ii) Proxy re-signatures, are used to update the tags when the group members change. This protocol provides user anonymity and integrity [Yu et al., 2014].
5) *Cipher-Text Policy Attribute Based Encryption (CP-ABE)*—This scheme provides access control in MCC environment and allows the mobile user to outsource computational processing to cloud from mobile device (reduced encryption and decryption operations), which helps to protect data from unauthorized access [Jin et al., 2015b]
6) *Secure Data Sharing in Clouds (SeDaSC)*—This method consists of three entities: user, cryptographic server, and cloud. (i) User provides data, list of group members, and access control list to cryptographic server. (ii) Upon receiving the data, cryptographic server encrypts the data using a symmetric key; which is divided into two keys: one for group members and the other for access control; (iii) The data (which is divided) is stored in the cloud (by cryptographic server). When a group member wants to download the data they

send the request (along with the symmetric key) to cryptographic server. After receiving the request, cryptographic server authenticates the member (to check whether the user is a valid member) and allows to decrypt, and download the data (stored in the cloud) [Ali et al., 2015].

Table 3. Comparisons of Data Security Solutions (cf. [Mollah et al., 2017]).

Works	**Proposed Schemes**	**Security Features**
Alqahtani *et al.*	Distributed multi-cloud storage, data encryption and data compression	Confidentiality
Wang *et al.*	Secure sharing, scalable watermarking and reed-solemon coding	Authentication and Confidentiality
Khan *et al.*	Block-based Sharing Scheme (BSS)	Confidentiality,Integrity
Yu *et al.*	Public auditing protocol	Integrity, Identity privacy protection
Jin *et al.*	Ciphertext-Policy Attribute based Encryption (CP-ABE) [algorithm]	Access Control
Ali *et al.*	Secure Data Sharing in Clouds (SeDaSC)	Confidentiality, AccessControl

Offloading Security Solutions. Here are few solutions to overcome offloading challenge:

1) *Data Partitioning*—This concept helps the mobile users to offload the data to remote and trusted entity from being exposed. This concept has three steps: (i) Dividing the data into two parts: sensitive, and non-sensitive data; (ii) Offloading the non-sensitive part to remote entity and executing the sensitive part on mobile device; (iii) Combining the results of remote entity and mobile device at mobile device end to obtain the final result [Al-Mutawa et al., 2014]. There is another solution called adaptive application partitioning, which uses the same concept but this concept is divides application (instead of data) [Dhanya and Kousalya, 2015].

2) *TinMan*—This concept ensures confidentiality apart from secure offloading (of data). In this concept, sensitive data is separated from regular mobile application which is later offloaded, and stored at a node (trusted). This node is installed on VM in trusted cloud. SSL (Secure Socket Layer) and TCP protocols are used during the offloading process and accessing sensitive data for security purpose [Xia et al., 2015].

Table 4. Comparisons of Offloading Security Solutions. (cf. [Mollah et al., 2017]).

Works	Proposed Schemes	Security Features
Al-Mutawa and Mishra	Data Partioning	Confidentility
Dhanya and Kousalya	Adaptive Application Partitioning	Secure Application Offloading
Xia *et al.*	TinMan	Confidentiality

Virtualization Security Solutions. To overcome the security problems related to virtualization, few frameworks have been proposed:

1) *Secure Mobile Cloud Platform (SMOS)*—It allow the users to securely clone the operating system and application to VM on cloud. Hardware virtualization technique allows isolation of data and application from operating system to ensure data security (on mobile device) and if the data needs higher security, file system extension is used (which helps the application to migrate to VM) [Hao et al., 2015].
2) *Security Framework*—This framework consists of two protocols: trusted VM launching protocol and domain based store data protection protocol. Trusted VM launching protocol is used before deploying guests VMs and domain based store data protection protocol is used to maintain confidentiality of the data (which is stored in remote storage by guest VMs) [Paladi et al., 2017].

Table 5. Comparisons of Virtualization Security Solutions (cf. [Mollah et al., 2017]).

Works	Proposed Schemes	Security Features
Hao *et al.*	Secure Mobile Cloud Platform (SMOC)	Confidentiality
Paladi *et al*	Security Famework	Confidentiality

Mobile Cloud Application Security Solutions.

1) *Secure Mobile Cloud (SMC)*—It allows the components in a network to securely communicate with each other. It also ensures integrity to the applications (during installation, updating, etc.) in mobile devices [Popa et al., 2013].
2) *Hybrid Attribute and Re-encryption Protocol*—These protocols help in securing mobile cloud applications. These two protocols use attribute based encryption, group keying, and re-encryption techniques. Attribute based encryption, distributes key generation responsibilities between mobile device and trusted entity. Group keying, provides a secret

key for a group which is only used by the group people and re-encryption encrypts the stored cipher [Tysowski et al., 2013].

3) *Secure Elastic Mobile Application Model*—The main focus of this framework is secured authentication, communication, and migration within components of mobile device and cloud. The key components of this model are: device elasticity manager, cloud manager and application manager: (i) Device elastic manager locates application components and select a secure path for communication (within components). (ii) Cloud manager allocates resources and maintain information about the components (computation, bandwidth etc.). (iii) Application manager (in the cloud end) install and launch application components in different cloud nodes [Zhang et al., 2009a].
4) Strict, Observable, Verifiable data and Execution *(STOVE)*—This model helps in executing untrusted mobile application securely by isolating the applications from other mobile device applications and operating system. It does not allow unauthorized data or application access [Tan et al., 2014].

Table 6. Comparisons of Mobile Cloud Application Security Solutions
(cf. [Mollah et al., 2017]).

work	**Proposed Scheme**	**Security Features**
Popa *et al*	Secure Mobile Cloud (SMC)	Integrity
Tysowski and Hasan	Hybrid Attribute and Re-encryption Protocol	Confidentiality
Zhang *et al*	Secure Elastic Mobile Application Model	Authentication
Tan *et al*	Strict, Observable, Verifiable data and Execution (STOVE)	Confidentiality

Mobile Devices Security Solutions. Security solutions for mobile device include solutions for physical threats, storage, malware, cloud-related etc.:

1) *Solutions for Physical Threats*—To avoid physical threats, application developers can add additional security (in application level). Where the users access sensitive data apart from that they can also make sure that the sensitive data is not stored in identity module card by the users (to avoid security problems). So, the question arises about the storage of data and that can be solved by cloud backup services so, even if the user loss his/her mobile device, they can still retrieve data from the backup service but these solutions does not resolve the problem of data misuse, to solve this Google has provided a special feature, which is, if the device is lost/stolen then the data inside the device can be cleared as well as it can be locked (remotely).

2) *Solutions for Malwares*—Malware attacks can be prevented by either cloud-based [Walls et al., 2015] or on-device security application [Imgraben et al., 2014] which detect and prevent mobile malware, control unauthorized access and protect privacy. Before preventing the malware, we need to detect, monitor, analyze and identify the malware, now let us see how these things help in preventing the malware:

   a) Detect—There are two ways to detect the malware, they are: static and dynamic analysis, where static analysis identifies suspicious strings using unpacking and decompiling the application process and dynamic analysis identifies malicious activities by running and installing the application on a device or on an emulator.

   b) Monitor—Monitoring techniques gather information like system calls, user activity, logs etc.

   c) Analyze—After gathering information we need to analyze it to see if there is any malware present. Analysis can be done by using some techniques like self-organizing map, data flow and control flow graphs etc.

   d) Identify—using intrusion detection system we can identify the malware and its type.

   The above techniques are mostly processed at cloud side as they utilize a lot of resources (some parts are processed at mobile device as well).

3) *Mobile Device Storage Issue Solution*—Mobile device storage issue can be solved by using cloud services to store the data within the cloud and the security issue (of data) can also be solved by encrypting the data and securing the encryption key by using Trusted Platform Module (this parallel protects confidentiality and integrity of the data stored in the cloud apart from the privacy).

4) *Cloud-Based Solutions*—As specified in solutions for malware, malicious applications prevention techniques are not feasible to run on mobile devices due to resource limitation. So, they are offloaded to the cloud. The cloud based solutions are feasible to address mobile device issues like:

   a) Secloud—It uses three components: mobile client agent, emulator, proxy server. The mobile client agent is an application that runs on mobile device, emulator acts as mobile device in the cloud through an image of VM of mobile devices, proxy servers makes mirror of mobile device network traffic. When the emulator detects security problems it informs the mobile client agent which either removes the infected files or informs the proxy server to close the network connection of the attacker [Zonouz et al., 2013].

   b) ThinAV—It uses two components: mobile client application and ThinAV server, where the mobile client application allows application offloading to ThinAV server after the process of offloading, ThinAV server sends the application to the third-party malware scanning where the application is scanned for malware and the result is sent to the mobile client application, which removes the infected files [Jarabek et al., 2012].

   c) Light Weight Anti-Malware Engine—It consist of three components: light weight agent, light weight anti-malware engine and in-cloud anti-malware engine. Here the light weight agent and light weight anti-malware engine analyze and detect the malware. If the malware cannot detect at these steps, then in-cloud anti-malware engine detects it (to take necessary actions). Due to these three components, this anti-malware engine becomes more efficient and faster than other approaches [Alam et al., 2014].

4. PRIVACY IN MCC

This section starts with privacy problems in MCC where it is divided into Subsection privacy risks which is further divided into privacy vulnerabilities and privacy threats.

4.1. Privacy Problems in MCC

In MCC, personal information collected by cloud provider is equivalent to a gold mine, whose privacy has begun to detriment and its long-term effects are yet to be seen. Cloud protects the data even if the device is lost or stolen i.e., the data stored in the cloud cannot be compromised easily, but there are still some privacy problems that occur due to the cloud [Chang et al., 2013]:

1) Cloud providers protect the data stored in the cloud. Users are not given control to store or protect their own data (in the cloud) due to which privacy related issues are in the hands of cloud providers.
2) What happens to the data if the data center is destroyed due to natural disasters?
3) Will the cloud provider provide strong encryption? If they do, will it be server-side or client-side?

Among these problem, the most serious problem occurs due to mobility that is, numerous applications are available, but are they safe? Do they collect private (important) information from the mobile devices to another party? Users are not aware of any of these problems and companies usually do not specify them to the users.

With the proliferation of mobile devices, the mobile cloud privacy problems will become more sophisticated and serious. Most of the problems occur due to ads but, it is not possible to cut down advertisements, as many free applications depend on advertisements and providing too much protection may change these free applications to fee-based applications. The possible solution is to give user more control, transparency, and choice. It is important that any personal data shared should have user’s consent, so that he/she can opt out of any data collecting program at any time [Chang et al., 2013].

Users are provisioned with application and services over mobile networks, which are designed in secured MCC platform. This provisioning helps mobile cloud to take advantage of benefits of Cloud Computing in monitoring, security detection, and malware prevention which does not mean that the application and services are out of malware danger, it only means that it is difficult to manipulate service provider and their services. As the application and service reside in the cloud there is no need of client terminal protection. Apart from this, some on-device protection (like anti-virus, anti-malware, etc.) may still be considered an extra protection.

The following requirements of mobile and ubiquitous system satisfies user privacy
[Fahrmair et al., 2008]:

1) Protection against misuse
2) Identification of pirated datasets
3) Adjustment of law
4) Ease of use

These are some of the privacy problems suggested by [Mollah et al., 2017]:
User's data are processed and shifted from mobile devices to cloud servers. These servers are located at different places in the world which makes it difficult for the user to maintain the data, thus cloud providers own, maintain, and protect mobile user's data. This raises a lot of privacy problems. It is important for the user to know about the location of data as law differ from country to country.

Several unsafe mobile applications collect user's personal information, which may be used illegally. This violates user's privacy.

The main feature of mobile application which differ from PC is context awareness (enabled by the sensor) it helps the service provider to provide the requested service to the user. Some of the location based services and applications increase privacy concerns, as many applications need user's location information to send back the requested service (like restaurants, coffee shop, etc.).

4.1.1. Privacy Threats

The current security concern in mobile cloud is threats to smartphone platforms which are classified into three major categories [Chang et al., 2013]:

Physical Threats. Attackers usually access data or application from borrowed, lost or stolen mobile devices. Although mobile devices are equipped with pin or password based lockout capabilities, there are numerous ways to unlock the mobile device. The application installed on mobile devices often provide direct and automated access to cloud services and data.

1) *Challenge*—When a device is lost or stolen, SIM card(s) is removed. The attacker tries to unlock the phone by reinserting a malicious SIM, which opens the gate for the attacker to access the data stored in the device.
2) *Possible Solutions*—When sensitive data is being accessed (using a software), there is a need for the developer's to add an extra layer of security at application level to avoid data tampering. They should also make sure not to store any important data (on the SIM) in the device. On cloud side, data should be encrypted for security. By taking the above precautions it would get difficult for the attacker to retrieve the data, even if the device gets

lost or stolen. The user (who lost the device) can always recover his data from the cloud using backup service. Apart from these methods, more advanced techniques like eye recognition, etc., can be added as an extra layer of protection (second authentication method).

Threats to Mobile Network Security. Users gain access to phone services, internet services, etc., through 3G, 4G, Wi-Fi, and Bluetooth. All network types are prone to security problems but when compared to wired networks, wireless networks are prone to more attacks. Some of the wireless network attacks are: eavesdropping, phishing, man-in-the-middle, etc.

1) *Challenge*—Using malicious software, downloading data from unsafe network, etc., can compromise the network security, which opens the gate for the attackers to access sensitive data.
2) *Possible Solutions*—There are some measures to prevent unauthorized access:
    a) Educating the user about the right way of using the network.
    b) Using one time passwords, two-factor authentication etc.
    c) Giving controls to the user, to personalize configuration profile.
    d) Need to control and protect the flow of information between mobile device and cloud storage.

4.2. Privacy Solutions in MCC

These are some of privacy solution for the problems suggested by [Mollah et al., 2017]:

Data Privacy. An approach was proposed by Pasupuleti et al., which uses probabilistic public key encryption technique and ranked keyword searching algorithm [Cao et al., 2014] to preserve privacy. Probabilistic public key encryption, encrypts both data and index. The user makes use of an index for file collection before sending it to the cloud (for storing). To access the stored data, user produces trapdoor for keywords and sends it to the cloud. Cloud starts to search for list of matched entries and its encrypted relevance which is later sent back to the user using ranked sequence based on relevance score. After receiving the data, the user decrypts it to retrieve original data.

Data Query Privacy. There are two data query privacy preserving approaches:

1) *Privacy Assured Substructure Similarity Query* [Zhang et al., 2014b]—This data query consists of three algorithms: (i) secure index construction; (ii) Trapdoor generation; and (iii) Query processing. Secure index construction encrypts the data (to protect it), while the other two algorithms performs trapdoor generation and privacy assured calculations respectively.
2) *Data Query Privacy for Mobile Mashup* [Owens and Wang, 2013]—This data query consists of two mechanisms: (i) Server-side; and (ii) Mobile client side. In server side data privacy within communication, between mashup server, and mobile client side are protected by dynamically creating VMs as proxies. In mobile client side, data collection and aggregation

procedures are protected from eavesdroppers by migrating (live) application level VMs to cloud.

Location Privacy. Several efforts have been made to protect location privacy. K-anonymity [Sweeney 2002], caching aware dummy selection algorithm [Niu et al., 2015], LP-doctor, etc., are some of the models used to protect location privacy. Among these LP-doctor is the most popular model [Fawaz et al., 2015].

LP-doctor is a fine grained location access control tool used to prevent location privacy threats. It allows the user to utilize operating system based location access control without modifying application layer or operating system. LP-doctor is divided into several components:

1) *Application Session Manager*—Monitors launch and exit of application events to make location anonymous.
2) *Policy Manager*— It applies any one of the three actions: block, allow and protect, on an application specified by the user, this is called privacy policy (specially for currently visited place and launched application).
3) *Place Detector*—Monitor's user's current location.
4) *Mobility Manager*—It updates user's location when the user changes his/her location.
5) *Threat Analyzer*—It decides whether the application is allowed to access the location or not. It depends on policy manager.
6) *Anonymization Actuator*—It depends on threat analyzer, when the threat analyzer decides to protect the location information, anonymization actuator take necessary action by adding a fake location to anonymize the location.

Table 7. Comparisons of Privacy Solutions. (cf. [Mollah et al., 2017]).

Works	**Proposed Schemes**	**Security Features**	**Scalability**
Pasupuleti *et al.*	Probabilistic Pubic key Encryption and Ranked keyword Searching Algorithm	Data Privacy	High
Zhang *et al.*	Privacy Assured Substructure Similarity Query (PASSQ)	Data Query Privacy	Moderate
Qwens and Wang	Data Query privacy Preserving for Mobile Mashups	Data Query Privacy	Low
Fawaz *et al.*	LP-doctor	Location Privacy	Moderate

5. INTERTWINED SECURITY AND PRIVACY IN MCC

The common intertwined security and privacy issues in MCC are discussed in this section.

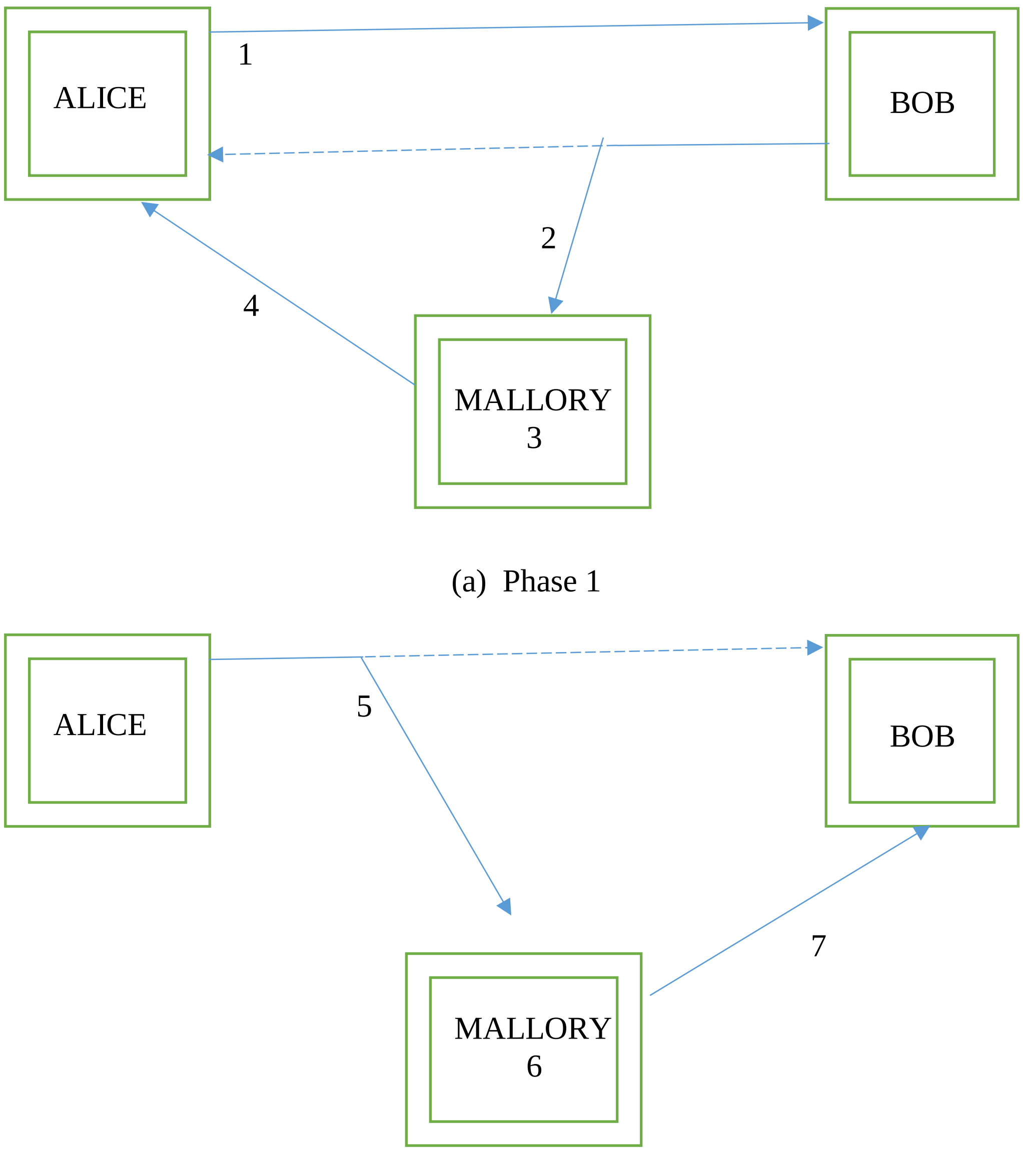
Let us see how they both get compromised simultaneously due to these issues. A few examples follow.

Whaling Attack. The whaling attack [Rouse, 2014b] is a type of fraud that targets high-profile end users. The goal is to trick them into disclosing personal or corporate information through social engineering, email spoofing and content spoofing. This attack might start with an illegitimate email message encouraging a high-ranking company employee to visit a fake web page. If the attacked executive is fooled into thinking that the web page is legitimate, she visits the web page. In the second phase of the whaling attack the illegitimate web page might ask her for her login name and password. The completion of the second step of whaling attack by the employee results in stealing username and password. In the third phase, attacker uses stolen username and password to authenticate a legitimate web page (as an authorized user) to steal important information such as company's security system details, client details, payroll, personal details (her account details, SSN), etc. [Giandomenico, 2017].

In this attack both security and privacy get compromised simultaneously. Security is compromised in all three phases. In the first phase, attacker uses social engineering to compromise security (only) by spoofing, by convincing the employee to access the fake web page. However, she should not be blamed. First, email was very believable and the fake web page precisely mimicked the original web page. Second, in an ideal world the outbound traffic would be controlled by an outbound access lists [Permitting or Denying Network Access, 2017] and the fake web page would not be on this list. In the second phase, it is compromised due to violation of confidentiality (as she provides her username and password). In the third phase, it is compromised due to passing authentication with the real username and password.

Privacy is compromised in the third phase due to the violation of confidentiality (the information is stolen as the control of access via login and password is compromised).

Man-in-the-Middle Attack. It is an attack where an attacker actively monitors, captures, and controls communication between two parties (transparently to them) [Lahon, 2017]. Suppose that Alice and Bob communicate with each other through email and Mallory (the attacker) wants to intercept the conversation (to eavesdrop) and deliver a falsified message to Bob. In the first phase of this attack, Alice asks Bob for his public key (Step 1). The key sent by Bob to Alice is intercepted by Mallory (man-in-the-middle attack begins) (Step 2). Mallory forges the message (Step 3) and sends the forged message to Alice that purports to come from Bob, but instead includes Mallory's public key (Step 4). In the second phase, Alice encrypts her message with Mallory's public key (believing that this is Bob's public key), and sends the enciphered message to Bob, e.g.: "Meet me at the coffee shop at 5 p.m." (Step 5). Mallory intercepts this message and deciphers it using his private key. Then, Mallory alters the message sent by Alice to: "Meet me at the coffee shop at 6 p.m." and enciphers it using Bob's public key (Step 6). Mallory sends the message to Bob (Step 7). Bob receives the message, believes that it came from Alice and comes to the coffee shop at 6 p.m. He misses Alice who came at 5 p.m. and left after waiting for him for 15 minutes.



(a) Phase 1

(b) Phase 2

Figure 19. Phases of Man-in-the-Middle Attack.

In this attack both security and privacy get compromised simultaneously. Security is compromised in two phases. In the first phase, attacker intercepts the conversation which compromises confidentiality, as the information is disclosed to the attacker; confidentiality is here a security aspect. In the second phase, it is compromised due to message falsification, which is an integrity breach (another aspect of security).

Privacy is compromised in the second phase by stealing information (about the meeting), which is a compromise of confidentiality; confidentiality is here a privacy aspect.

Attacks on Location Service. Users enable location services (such as GPS, GLONASS or Galileo) in their mobile devices for convenience. Attackers make use of GPS spoofing to steal the data; this attack attempts to deceive a GPS receiver by broadcasting incorrect GPS signals, structured to resemble a set of normal GPS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time [Thomson, 2013].

Now let us see how an attacker tricks a ship captain into changing the correct ship's course by using GPS spoofing. The ship navigation is based on GPS signals broadcast from orbiting satellites. In the first phase, the attacker uses his GPS spoofing device to transmit fake GPS signals towards the ship. The attacker increases the power of the spoofing signals until they are stronger than the satellite signals thus gaining control of the ship navigation system. Now the attacker tries to displays incorrect location information for the Capitan. This is stealthy, no alarms are triggered. In the second phase, the Capitan changes the ship course according to the navigation data (which is displayed incorrectly). Now the ship is on a new course, where its position is a few degrees off its original course, heading towards pirates' speedboats.

In this way both security and privacy get compromised simultaneously. Security is compromised in two phases. In the first phase, security is compromised due to violation of authentication (non GPS signals taken as GPS signals). In the second phase, security is compromised due to violation of integrity (correct GPS data replaced with "false GPS" data) and violation of confidentiality (navigation system data is being accessed by the attacker, which gave him control to send incorrect signals to the Captain).

Privacy is compromised in the second phase, due to loss of confidentiality (as the control of access is compromised).

Data Theft. Pretexting [Social Engineering, Wikipedia, 2018] is a form of social engineering, which is defined as "The act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance [that] the victim will divulge information or perform actions that would be unlikely in ordinary circumstances [Faraz, 2014]. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target [Pretexting, FTC, 2018]."

Consider a scenario [Nadeem, 2015], where an attacker Mallory impersonates a bank manager Bob to an account holder Alice. In the first phase, Mallory tries to establish trust with Alice. To this end, Mallory uses some historical facts he gathered earlier. For example, he says "Hi, I am Bob Jones, the manager of Our Neighborhood Bank. I have met you last November, when you came in for a bank loan. Today I can offer you better interest rate on your savings." In the second phase, Mallory (after gaining Alice's trust) gathers Alice's username, account number, SSN, etc., pretending that he needs this information for verification of Alice's identity, to give her the better interest rate on her savings.

In this way both security and privacy are compromised simultaneously. Security is compromised in two phases. In the first phase, the attacker uses social engineering to compromise the security due to violation of authentication (by impersonation). In the second phase, security is compromised due to violation of confidentiality (as data is stolen by the attacker); confidentiality is here a security aspect.

Privacy is compromised in the second phase, due to violation of confidentiality (data is stolen); confidentiality is here a privacy aspect.

6. CONCLUSIONS OF MCC

Mobile applications are demanding and play an important role in today's modern world. In this survey firstly we discussed Cloud Computing and Mobile Computing, which are integrated into Mobile Cloud Computing (MCC) technology. Mobile Cloud Computing aims to empower mobile users by providing a seamless functionality regardless of resource limitations of mobile devices.

Secondly, the survey presents an overview of Mobile Cloud Computing, which includes architecture and applications of Mobile Cloud Computing. It concentrates on security and privacy problems (threats) along with their related solutions, classifying these problems (threats) and solutions as either security-related, privacy-related, or intertwined (no solutions for the intertwined problems were identified in the literature).

This research field is still immature and not explored in depth. Many security and privacy problems are still under research. Overcoming these problems should fulfill the promise of MCC.

REFERENCES

[Al-Gburi et al., 2018] A. Al-Gburi, A. Al-Hasnawi, L. Lilien, “Differentiating Security from Privacy in Internet of Things- A Survey of Selected Threats and Controls,” Chapter 9 in K. Daimi, *Computer and Network Security Essentials*, Springer, Cham, Switzerland, pp. 153-172.

[Al-Hasnawi and Lilien, 2016] A. Al-Hasnawi, L. Lilien, "Privacy Services and Mechanisms (slides),” Department of Computer Science, Western Michigan University.

[Al-mawee, 2015] Wassnaa Al-mawee, “Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey,” Master’s Thesis, Department of Computer Science, Western Michigan University, pp. 1-39.

[Al-Muhtadi et al., 2002] J. Al-Muhtadi, A. Ranganathan, R. Campbell, M.D. Mickunas “A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments,” *Twenty-Second International Conference on Distributed Computing Systems Workshops*, pp. 2-6.

[Alqahtani et al., 2014] Hassan Saad Alqahtani, Ghita Kouadri-Mostefaou, “Multi-Clouds Mobile Computing for the Secure Storage of Data,” *IEEE/ACM Seventh International Conference on Utility and Cloud Computing*, pp. 495-496. **DOI:** 10.1109/UCC.2014.68.

[Ali et al., 2017] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Albert Y. Zomaya, “SeDaSC: Secure Data Sharing in Clouds,” *IEEE Systems Journal*, vol. 11(2), pp. 395-404.

[Al-Mutawa et al., 2014] Mohammad Al-Mutawa, Shivakanth Mishra, "Data partitioning: an approach to preserving data privacy in computation offload in pervasive computing systems,” *Tenth ACM symposium on QoS and Security for Wireless and Mobile Networks*, pp. 51-60. **DOI:** 10.1145/2642687.2642696.

[Alam et al., 2014] Shahid Alam, Ibrahim Sogukpinar, Issa Traore, Yvonne coady, “In-Cloud Malware Analysis and Detection: State of the Art,” *Seventh International Conference on Security of Information and Networks*, pp. 1-6. **DOI:** 10.1145/2659651.2659730.

[Online: 2016] “Amazon Simple Storage Service details.” Available at: https://aws.amazon.com/s3/.

[Bahl et al., 2012] Paramvir Bahl, Richard Y. Han, Li Erran Li, Mahadev Satyanarayanan, “Advancing the State of Mobile Cloud Computing,” *Third ACM Workshop on Mobile Cloud Computing and Services*, pp. 21-28.

[Online: 2016] “Base Station.” Available at: https://www.google.com/search?q=base+station&oq=base+&aqs=chrome.2.69i57j69i60j69i59j69i60l2j0.3272j0j7&sourceid=chrome&ie=UTF-8.

[Bonneau et al., 2010] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *IEEE Symposium on Security and Privacy*, pp. 553-567. **DOI:** 10.1109/SP.2012.44.

[Cao et al., 2014] Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25(1), pp. 222-233.

[Chang et al., 2013] Ruay-Shiung-Chang, Jerry Gao, Volker Gruhn, Jingsha He, George Roussos, Wei-Tek Tsai, "Mobile Cloud Computing Research- Issues, Challenges and Needs," *IEEE Seventh International Symposium on Service-Oriented System Engineering*, pp. 442- 453.

[Christensen, 2009] Jason H. Christensen, "Using RESTful Web-Services and Cloud Computing to Create Next Generation Mobile Applications," *Twenty-Fourth ACM SIGPLAN Conference Companion on Object Oriented Programming Systems Languages and Applications*, pp. 627-634. DOI: 10.1145/1639950.1639958.

[Chun et al., 2011] Byung-Gon Chun, Sunghwan Ihm, Petros Maniatis, Mayur Naik, Ashwin Patti, "Clone Cloud: Elastic Execution between Mobile Device and Cloud," *Sixth Conference on Computer Systems*, pp. 301-314. **DOI:** 10.1145/1966445.1966473.

[Online: 2016] "Cloud Computing." Available at: https://en.wikipedia.org/wiki/Cloud_computing.

[Online: 2016] "Compute Node." Available at: http://h17007.www1.hpe.com/docs/enterprise/servers/cloudsystem/webhelp/content/s_about-vmhost-isc.html.

[Cox, 2011] Preston A. Cox, "Mobile Cloud Computing: Devices, Trends, Issues, and the Enabling Technologies," *IBM Developer Works*. Available at: https://www.ibm.com/developerworks/cloud/library/cl-mobilecloudcomputing/.

[Cuervo et al., 2010] Eduardo Cuervo, Aruna Balasubramanian, Dae-ki Cho, Alec Wolman, Stefan Saroiu, Ranveer Chandra, Paramvir Bahl, "MAUI: Making Smartphones Last Longer with Code Offload," *Eighth International Conference on Mobile Systems, Applications, and Services*, pp. 49-62. **DOI**: 10.1145/1814433.1814441.

[Davani, 2011] Faraz davani, "HP Pretexting Scandal," SCRIBD, pp. 30. Available at: https://www.scribd.com/doc/62262162/HP-Pretexting-Scandal.

[Dhanya and Kousalya, 2015] N.M. Dhanya, G. Kousalya, "Adaptive and Secure Application

Partitioning for Offloading in Mobile Cloud Computing," Chapter 5 in Jemal H. Abawajy, Sougata Mukherjea, Sabu M. Thampi, Antonio Ruiz-Martinez, *International Symposium on Security in Computing and Communication*, vol. 536, pp. 45-53.

[Dinh et al., 2011] Hoang T. Dinh, Chonho Lee, Dusit Niyato, Ping Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13(18), pp. 1587-1611. **DOI**: 10.1002/wcm.1203.

[Online: 2016] "Drive-by download." Available at: https://en.wikipedia.org/wiki/Drive-by_download.

[Online: 2016] "Elasticity." Available at: https://www.google.com/search?rlz=1C1GCEA_enUS751US751&ei=ep_4WcvUHuLdjwShwoawBQ&q=elasticity+definition&oq=elasticity&gs_l=psyab.1.1.35i39k1l2j0i131k1j0i67k1j0i131k1j0i67k1j0j0i131k1l2j0i67k1.16340.22211.0.27132.17.11.3.0.0.0.144.1074.0j9.9.0....0...1.1.64.psy-ab..5.12.1080...0i20i263k1.0.0QVXcYi21w0.

[Fahrmair et al., 2007] Michael Fahrmair, Wassiou Sitou, and Bernd Spanfelner "Security and privacy rights management for mobile and ubiquitous computing," *Workshop on Ubicomp Privacy*, pp. 97-108.

[Fawaz et al., 2015] Kassem Fawaz, Huan Feng, and Kang G. Shin "Anatomization and Protection of Mobile Apps' Location Privacy Threats," *Twenty-Fourth USENIX Security Symposium*, pp. 753-768.

[Fernando et al., 2013] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, "Mobile Cloud Computing: A survey," *Future Generation Computer Systems*, vol. 29(1), pp. 84-106.

[Giandomenico, 2017] Nena Giandomenico, "What is Whaling attack?" *Digital Guardian*. Available at: https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks.

[Guan et al., 2011] Le Guan, Xu Ke, Meina Song, Junde Song, "A Survey of Research on Mobile Cloud Computing," in IEEE/ACIS Tenth *International Conference on Computer and Information Science*, pp. 387-392. **DOI**: 10.1109/ICIS.2011.67.

[Hao et al., 2015] Zijiang Hao, Yutao Tang, Yifan Zhang, Ed Novak, Nancy Carter, Qun Li "SMOC: A Secure Mobile Cloud Computing Platform," *IEEE Conference on Computer Communications*, pp. 2668-2676.

[Harbitter and Menasce, 2011] Alan Harbitter, Daniel A. Menasce, "The Performance of Public Key-Enabled Kerberos Authentication in Mobile Computing Applications," *Eighth ACM Conference on Computer and Communications Security*, pp. 78-85.
DOI: 10.1145/501983.501995.

[Hutnik, 2012] Alysa Zeltzer Hutnik, “Location-Based Services: Why privacy “Dos and Don’ts” Matter,” *iapp*. Available at: https://iapp.org/news/a/2012-03-08-location-based-services-why-privacy-dos-and-donts-matter/.

[Jones, 2017] Jake Jones, “Edge Computing: The Cloud, the fog and the Edge,” *SolidRun*. Available at: https://www.solid-run.com/edge-computing-cloud-fog-edge/.

[Jarabek et al., 2012] Chris Jarabek, David Barrera, John Aycock, “ThinAV: Truly Lightweight Mobile Cloud-based Anti-malware,” *Twenty-Eighth Annual Computer Security Applications Conference*, pp. 209-218. **DOI:** 10.1145/2420950.2420983.

[Jin. Y. et al., 2015b] Yu Jin, Chuan Tian, Heng He, Fan Wang, “A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing,” *IEEE Fifth International Conference on Big Data and Cloud Computing*, pp. 172-179. **DOI:** 10.1109/BDCloud.2015.57.

[Jonathan, 2013] Bar-Magen Numhauser, “Fog Computing introduction to a New Cloud Evolution,” *Silenced Scriptures: landscape as Historiography*, *Spain*, pp. 111-126. ISBN: 978-84-15595-84-7.

[Khalil et al., 2014] Issa Khalil, Abdallah Khreishah, Muhammad Azeem, “Consolidated Identity Management System for secure mobile cloud computing,” *Journal of Computer Networks*, vol. 65, pp. 99-110.

[Khan et al., 2014a] Abdul Nasir Khan, Laiha Mat Kiah, Mazhar Ali, Shahaboddin Shamshirband, “BSS: Block-based Sharing Scheme for secure data storage services in mobile cloud computing,” *The Journal of SuperComputing*, vol. 70(2), pp. 946-976. **DOI:** 10.1007/s11227-014-1269-8.

[Khan et al., 2014b] Atta ur Rehman Khan, Mazliza Othman, Sajjad Ahmad Madani, Samee Ullah Khan, “A Survey of Mobile Cloud Computing Application Models,” *IEEE Communication Surveys and Tutorials*, vol. 16(1), pp. 393-413.

[Kosta et al., 2012] Sokol Kosta, Andrius Aucinas, Pan Hui, Richard Mortier, Xinwen Zhang, “ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading,” *Proceedings IEEE INFOCOM*, pp. 945-953. **DOI**: 10.1109/INFCOM.2012.6195845.

[Krishnan, 2017] Rama Krishnan Krishnan “Security and Privacy in Cloud Computing,” A Survey paper of Western Michigan University, Western Michigan University, Kalamazoo, Michigan, fall 2017. Available at: http://scholarworks.wmich.edu/masters_theses/919/.

[Lahon. M, 2017] “What is Man in the middle attack?” *Crack IT Down*. Available at: http://www.crackitdown.com/2017/11/what-is-man-in-middle-attack-best-way.html.

[Lampe et al., 2012] Ulrich Lampe, Melanie Siebenhaar, Apostolos Papageorgiou, Dieter Schuller, Ralf Steinmetz, "Maximizing Cloud Provider Profit from Equilibrium Price Auctions," *IEEE Fifth International Conference on Cloud Computing*, pp. 83-90. **DOI:** 10.1109/CLOUD.2012.19.

[Li et al., 2011] Huixi Li, Hao Li, "A Research of Resource Provider-Oriented Pricing Mechanism Based on Game Theory in Cloud Bank Model," *International Conference on Cloud and Service Computing*, pp. 126-129.

[Lilien et al., 2010] Leszek Lilien, Adawia Al-Alawneh, Lotfi Ben Othmane, "The pervasive trust foundation for security in next generation networks," *The New Security Paradigms Workshop*, pp. 120-142.

[Li Yang, 2017] Li Yang, "Mobile Threats Examples". Available at: http://www.utc.edu/faculty/li-yang/5.mobile threats attacks.pptx.

[Lopez et al., 2015] Pedro Garcia Lopez, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino, Adriana lamnitchi, Marinho Barcellos, Pascal Felber, Etienne Riviere, "Edge-centric Computing: Vision and Challenges,"*ACM SIGCOMM Computer Communication Review*, vol. 45 (5), pp. 37–42.

[Malik et al., 2013] Sapna Malik, MM Chaturvedi, "Privacy and Security in Mobile Cloud Computing: Review," *International Journal of Computer Applications*, vol. 80(11), pp. 20-26.

[Online: 2017] "Malware." Available at: https://en.wikipedia.org/wiki/Malware.

[Mell and Grance, 2009] Peter Mell, Tim Grance, "The NIST Definition of Cloud Computing," *National Institute of Standard and Technology, Information Technology Laboratory,* vol. 15, pp. 1-7.

[Mollah et al., 2017] Muhammad Baqer Mollah, Md. Abdul Kamal Azad, Athanasios Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38-54.

[Online: 2017] "Mobile Computing." Available at: https://en.wikipedia.org/wiki/Mobile_computing.

[Online: 2017] "Mobile Cloud Computing." Available at: https://en.wikipedia.org/wiki/Mobile_cloud_computing.

[Nadeem, 2015] M Salman Nadeem, "Social Engineering: what is pretexting?" *Secure and private email service*. Available at: https://blog.mailfence.com/pretexting.

[NEC Company, Ltd., Information, and Privacy Commissioner, 2010]

"Modelling Cloud Computing Architecture without Compromising Privacy: A privacy by design Approach," Ontario, Canada. Available at: https://pdfs.semanticscholar.org/ec67/172f29d738fc63c17f7e68ec48a3f7d74bac.pdf.

[Niu et al., 2015] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, Hui Li, "Enhancing Privacy through Caching in Location-Based Services," *IEEE Conference on Computer Communications*, pp. 1017-1025.

[Owens and Wang, 2013] Rodney Owens, Weichao Wang, "Preserving Data Query Privacy in Mobile Mashups through Mobile Cloud Computing," *Twenty-Second International Conference on Computer Communications and Networks*, pp. 1-5. **DOI:** 10.1109/ICCCN.2013.6614169.

[Padron, 2016] Kristy Padron, "LibGuides: Guide to Science Information Resources: Backward and Forward," *FAU Libraries*, Reference Searching," Available on: http://libguides.fau.edu/c.php?g=325509&p=2182112.

[Paladi et al., 2017] Nicolae Paladi, Christian Gehrmann, Antonis Michalas, "Providing User Security Guarantees in Public Infrastructure Clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419.

[Pasupuleti et al., 2016] Syam Kumar Pasupuleti, Subramaniam Ramalingam, Rajkumar Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *Journal of Network and Computer Applications*, vol. 64, pp. 12-22.

"Permitting or Denying Network Access", *Cisco ASA 5500 Series Configuration Guide using the CLI*, pp. 1-8. Available at: https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_nw.pdf.

[Popa et al., 2013] Daniela Popa, Marcel Cremene, Monica Borda, Karima Boudaoud, "A Security Framework for Mobile Cloud Applications," *Eleventh Roedunet International Conference*, pp. 1-4. **DOI:** 10.1109/RoEduNet.2013.6511724.

[Online: 2017] "Pretexting: Your personal Information Reveled," *Federal Trade Commission.* Available at: https://www.consumer.ftc.gov/.

[Qi et al., 2012] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review, Trend and Perspectives," *IEEE Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pp. 195-202.

[Rahimi et al., 2014] M. Reza Rahimi, Jian Ren, Chi Harold Liu, Athanasios V. Vasilakos, Nalini Venkatasubramanian, "Mobile Cloud Computing: A Survey, State of Art and Future Directions," *Mobile Networks and Applications*, vol. 19(2), pp. 133-143. DOI: 10.1007/s11036-013-0477-4.

[Rajasekar et al., 2013] S. Rajasekar, P. Philominathan, V. Chinnathambi, "Research Methodology." Available at: https://arxiv.org/pdf/physics/0601009.pdf.

[Redekar et al., 2014] Pragati Redekar, Rakesh Rajini, "Towards Mobile Cloud Computing," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, vol. 3(10), pp. 3335-3338.

[Online: 2017] "Regional Data Center." Available at: https://en.wikipedia.org/wiki/Data_center.

[Online: 2017] "Research Methodology." Available at: http://www.businessdictionary.com/definition/research-methodology.html.

[Rouse, 2017a] Margaret Rouse, "Storage Node." Available at: http://searchstorage.techtarget.com/definition/storage-node.

[Rouse, 2014b] Margaret Rouse, "Whaling Attack", *Techtarget*. Available at: http://searchsecurity.techtarget.com/definition/whaling.

[Sanaei et al., 2013] Zohreh Sanaei, Saeid Abolfazli, Abdullah Gani, Rajkumar Buyya, "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges," *IEEE Communication Surveys & Tutorials*, Vol. 16(1), pp. 369-390.

[Satyanarayanan et al., 2009] Mahadev Satyanarayan, Paramvir Bahl, Ramon Caceres, Nigel Davies, "The case for VM-based cloudlets in Mobile Cloud Computing," *IEEE Pervasive Computing*, vol. 8, pp. 14-23.

[Online, 2017] "Scalability." Available at: https://www.google.com/search?q=scalability+definition&rlz=1C1GCEA_enUS751US751&oq=scalability+&aqs=chrome.2.69i57j0j35i39j0l3.6655j0j7&sourceid=chrome&ie=UTF-8.

[Shahzad et al., 2014] Abid Shahzad, Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing," *International Journal of Grid and Distributed Computing*, vol. 6(6), 2013, pp. 37-50. Available at: http://dx.doi.org/10.14257/ijgdc.2013.6.6.04.

[Online: 2017] "Social Engineering," *Web Application Security Center*. Available at: https://www.incapsula.com/web-application-security/social-engineering-attack.html.

[Online: 2017] "Spyware (Wikipedia)," "Spyware (FTC)." Available at: https://en.wikipedia.org/wiki/Spyware and https://www.ftc.gov/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-other-software.

[Suo et al., 2013] Hui Suo, Zhuohua Liu, Jiafu Wan, Keliang Zhou, "Security and Privacy in Mobile Cloud Computing," *Ninth International Wireless Communications and Mobile Computing Conference*, pp. 655-659. **DOI:** 10.1109/IWCMC.2013.6583635.

[Sweeney, 2002] Latanya Sweeney, "K-Anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10(5), pp. 557-570.

[Tan et al., 2014] Jiaqi Tan, Rajeev Gandi, Priya Narasimhan, "STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications," *IEEE Sixth International Conference on Cloud Computing Technology and Science*, pp. 644-649. **DOI:** 10.1109/CloudCom.2014.116.

[Thomson, 2013] Lain Thomson, "Texas Students Hijack Superyacht with GPS-spoofing luggage," *The Register*. Available at: https://www.theregister.co.uk/2013/07/29/texas_students_hijack_superyacht_with_gpsspoofing_luggage.

[Tysowski et al., 2013] Piotr K. Tysowski, M. Anwarul Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds," *IEEE Transactions on Cloud Computing*, vol. 1(2), pp. 172-186. **DOI:** 10.1109/TCC.2013.11.

[Vikas et al., 2014] S. Solanke Vikas, Katgaonkar Pawan, A. Kulkarni Gurudatt, Gupta Shyam, "Mobile Cloud Computing: Security Threats," *International Conference on Electronics and Communication Systems*, pp. 1-4. **DOI:** 10.1109/ECS.2014.6892511.

[Wang et al., 2014a] Honggang Wang, Shaoen Wu, Min Chen, Wei Wang, "Security Protection between Users and the Mobile Media Cloud," *IEEE Communications Magazine: Security in Wireless Multimedia Communications*, pp. 73-79.

[Wang et al., 2012b] Wei Wang, Baochun Li, Ben Liang, "Towards Optimal Capacity Segmentation with Hybrid Cloud Pricing," *Thirty-Second IEEE International Conference on Distributed Computing Systems*, pp. 425-434. **DOI**: 10.1109/ICDCS.2012.52.

[Wang et al., 2014c] Yating Wang, Ing-Ray Chen, Ding-Chau Wang, "A Survey of Mobile Cloud Computing Applications: Perspective and Challenges," *Wireless Perspective Communication*," vol. 80, pp. 1607-1623. **DOI:** 10.1007/s11277-014-2102-7.

[Xia et al., 2015] Yubin Xia, Yutao Liu, Cheng Tan, Mingyang Ma, Haibing Guan, Binyu Zang, Haibo Chen, "TinMan: Eliminating Confidential Mobile Data Exposure with Security Oriented Offloading," *Tenth European Conference on Computer Systems*, article no. 27, pp. 1-16. **DOI:** 10.1145/2741948.2741977.

[Yu et al., 2014] Yong Yu, Yi Mu, Jianbing Ni, Jiang Deng, Ke Huang, "Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage," *International Conference on Network and System Security,* vol. 8792, pp. 28-40.

[Zafer et al., 2012] Murtaza Zafer, Yang Song, Kang-Won Lee, "Optimal Bids for Spot VMs in a Cloud for Deadline Constrained Jobs," *IEEE Fifth International Conference on Cloud Computing*, pp. 75-82. **DOI:** 10.1109/CLOUD.2012.59.

[Zaman et al., 2013] Sharrukh Zaman, Daniel Grosu, "A Combinatorial Auction-Based Mechanism for Dynamic VM Provisioning and Allocation in Clouds," *IEEE Transactions on Cloud computing,* vol. 1(2), pp. 129-141.

[Zhang et al., 2009a] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong "Securing Elastic Applications on Mobile Devices for Cloud Computing," *Proceedings of ACM Workshop on Cloud Computing Security*, pp. 127-134. **DOI:** 10.1145/1655008.1655026.

[Zhang et al., 2014b] Yingguang Zhang, Sen Su, Yulong Wang, Welfeng Chen, Fangchun Yang, "Privacy-assured substructure similarity query over encrypted graph-structured data in cloud," *Journal of Security and Communication Networks,* vol. 7(11), pp. 1933-1944.

[Zonouz et al., 2013] Saman Zonounz, Amir Houmansadr, Robin Berthier, Nikita Borisov, William Sanders, "Secloud: A cloud-based comprehensive and lightweight security solution for smartphones," *Journal of Computer and Security,* vol. 37, pp. 215-227. **DOI:** 10.1016/j.cose.2013.02.002.