A Review in Security Issues and Challenges on Mobile Cloud Computing (MCC)

Shirin Abdul.S . Muhseen
Informatics Institute for Postgraduate Studies (IIPS)
Iraqi Commission for Computers and Informatics (ICCI)
Baghdad, Iraq
shirin7_2002@yahoo.com

Amer S. Elameer
Informatics Institute for Postgraduate Studies (IIPS)
Iraqi Commission for Computers and Informatics (ICCI)
Baghdad, Iraq
amerelameer@yahoo.com

***Abstract* - cloud computing exhibit itself a rising innovation in IT world, which provides a new diagram of activity that empowers organizations to use virtual products, applications and equipment assets with no in any up-front investment. Few years later with the great advancements in cloud computing and vast enhancement of portable programs, further evolution is being expected in the form of Cloud Computing integration with mobile devices which gave birth to Mobile Cloud Computing (MCC) . Mobile cloud computing is obtaining the prominence of the among user of mobile device . it supplies a platform where transportable device users employ cloud services on transportable devices. The exploit of MCC minimizes the performance , compatibility and lack of resource issues in transportable device environment. Despite the hype of transportable cloud computing, the growth of movable cloud regular customers remained lesser than anticipations because of the risks related with security and confidentiality. These risks play a significant role in preventing organizations from αdopting the MCC environment. Major research is underway to reduce security issues, but much work remains to be done for create a secure MCC environment. This document represents a comprehensive review of MCC security issues and challenges**

Keywords:-- Cloud Computing (CC) ; MCC; Mobile Computing (MC) ; mobile Security Issues; Data Security in cloud.

I. INTRODUCTION

For deeper understand of mobile cloud computing MCC that needful get a complete comprehension on cloud computing (CC) . Cloud computing is an emerging technology that provides services and computing resources to customers through a public network specific to the network . Cloud computing services and infrastructure are possess by cloud service providers. Cloud Computing offers an innovative model for organization to use software applications, cloud storage and processing capabilities without investing in infrastructure. Compared to existing IT models, Cloud Computing offers a number of benefits like as scalability, flexibility, efficiency and non-core activities [1]. Regardless these excepcional benefits of Cloud Computing security is a big regard . According to a survey, published in 2009 by the International Data Corporation (IDC) [2], 74% of IT managers and Chief Information Officer (CIOs) think that security and privacy issues are the essential drawback preventing companies from adopting services on the cloud. The same year , a survey conducted by the Garter revealed that more than 70% of chief echnology officers (CTO) have expressed worry for data security and privacy issues in the cloud computing [3],

Cloud computing has been turned into the focal point of research center for both scholarly world and industry. through the methods for on-demand self-service and extendibility, cloud computing gives a series of services , for example, SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) , IaaS (lnfrastructure-as-a-Service) and so on. In this way, it is known as another generation of data advances. Then, with the fast advancement of mobile net and roving terminals, PDAs are increasingly supported by clients.

It is turning into a pattern to utilize portable terminals to arrival to the service give by the cloud. In this manner, MCC is rising out of the over hot technologies : (cloud computing and mobility) [4]

In view of the idea of cloud computing CC, mobile cloud computingMCC is characterized as a pattren for giving different IT resources and information services by the portable net through the methods for on-demand self-service mobile cloud computing is thee utilization of cloud computing in integration with portable devices.[5]

As per the study from Allied Business Intelligence, in excess of 2.4 billion clients will utilize a portable device to arrival to the cloud computing service for 2015, where it is winding up increasingly vital in our life then a few organizations offered agents versatile items in the cloud. For instance, Google display some cloud-based products for consumers and businesses.. The essential item among them is the Android OS for cell phones. as well Google has launched new application in light of portable terminal and cloud computing, e.g. geographic pursuit and Google Maps, Google streets.[6].

II. NEED OF SECURITY

Security is essential because mobile devices can encounter a variety of security threats when exposed to the outside world,

978-1-5386-9188-5/18/$31.00 ©2018 IEEE
DOI 10.1109/AiCIS.2018.00035

which can lead to viral attacks. When using mobile devices in cloud environments, users and / or application developers should be very careful with authentication and data / application integrity. Mobile security can be easily achieved with any security software installation, such as antivirus programs for mobile devices. The GPS causes privacy and LBS (location -based service) issues, in addition to providing the details of the current location, which is private information.

To protect the data, it is necessary to identify the possible threats and

challenges that demand to addressed such as privacy and security data replication , consistency , portability , scalability, availability cloud resources , unreliability , trust .through the implementation of appropriate countermeasures While designing secure systems, Security in a broad domain is regarding for important aspects of confidentiality, availability and integrity These important safety features, place to three major kinds of assets to protected : Data, Software and Hardware resources . these become the basic building blocks.

We can be classified issue of the security in Mobile cloud computing as:

- Mobile threats
- cloud Threats

The security related issues are additionally partitioned into the underneath given wide level classes

- Mobile cloud Infrastructure problem
- Mobile cloud connection channel problem

III. SECURITY THREATS AND COUNTERMEASURES

There is numerous difficulties have turned into an obstruction in the Rapid development of the MCC supporter. The challenges incorporating Frame or style in a uniform execution, limite scalability, unreliability, data redundancy, unreliabilitial cloud resources, portability (shortage of standard cloud provider), security and confidentiality.The challenges said above, that are faceing MCC [7] to draw in potential purchasers,the cloud service provider must spotlight on all security issues to give a totally secure enviornment . Notwithstanding the exploration gave. There are as yet several hazy areas which ought to be tended to addressed, for example, security and secrecy of client information on server (s) in the cloud, security dangers caused by various instrument and intrusion detection. As MCC depend on cloud computing , all security issues are inherit in MCC form the supplement limitations of mobile resources restriction devices . Because of the asset constraint, the proposed security algorithms for cloud computing the environmeeeent can not be run directly on a portable device.

There are a requirements for a lightweight security frame that gives security minimal connecting and processing costs on portable device. Figure 1 demonstrates the diverse security sevices that can be keep running in various layers to give a safe MCC environment. There is have to create security structure according to various confide level of cloud server and type of cloud server.

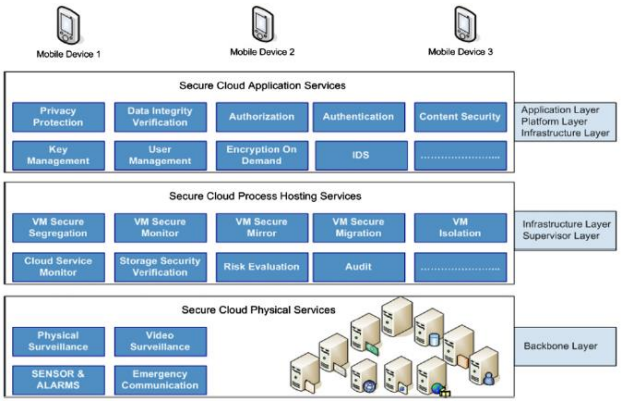

Fig-1: Security services on different layers.

We can executed privacy and Security services by the help of secure cloud applications in addition to security and privacy, providing secure cloud applications to the user adminstration, key management, encryption on demand ,intrusion detection, authentication, and license services to portable users. There is requirement for a secure link channel between cloud and the mobile device. secure routing protocols can be used to protect the connection channel among the portable device and cloud. Virtualization enhancement utilization of cloud resources but presents new security problem due to the shortage of perfect isolation of V.M hosted on a single server.

with the assistance of a cloud service monitorThe security problem forced by virtualization can handled to several scope with the help of V.M secure checking , mirror, and migration.Tosupply the transparent cloud environment , users of mobile device should have the facility for checking the security grade of the hosted services. The security grade should accept the user security requests and the flow on the running environment should be ordinary The checking can be done with The cloud sevice mointer check the security level and flows on the running environment. The security investigation for uploaded data in cloud can executable using a storage security verification service. Physical security in data center plays significant role for perform security and confidentiality. Physical security concern to prevent unauthorized personnel from gaining physical access resources of the cloud private organizations. it can be chieved with the help of security guards ,CCTV [8]

MCC has been a dynamic zone of research. despite of MCC is in the preparatory stages , there are limite surveys obtainable in several MCC domains [9] -. In [10] the writer disscue the mobile cloud computing architecture ,application and approaches so the author mention is just a single study managing security issues as a major aspect of the MCC review .

In [11], the writer display the examination of various app patterns in MCC and feature the difficulties of research regarding on the subject so the author not mention the

security challenge as major subject . writer in [12] studied MCC structures, app offloading and context aware services. principle target in the study exhibited in [9] alludes to mobile communcation and processing issues. The issues of mobile communcation are related with a low data transfer capacity, service accessibility, accessibility and heterogeneity. Computing issue is related together computing offloading, data access, security and context-aware mobile cloud services so the author mention the security challenge form kind of mobile device and wireless connection not mention on the detail

.This paper is different from others is focusing on the security problem for MCC, existing lightweight security frame are studied in detail, identifies the security parameters open privacy and security research questions in MCC, and the advancced taxonomy is presented.

IV. ANALYSIS STANDARD FOR SECURITY FRAMEWORKS

The MCC, security frameworks fall in two class : (a) application security frameworks and (b) data security frameworks. Because of numerous of the security structures gave that adapt the security in appliation/information created and manipulated on aportable device or cloud servers, which that involve security parts in mobile app.s or mobile app type that utilizations cloud resources to expand the limit of portable device.
for the successful deployment of security framework in an MCC environment .the computational demands , scalability and assumptions play important role On the other hand, storing files on a server in the cloud without uncovering or exposing any information.is more interested for mobile users
Security frameworks should also ensure confidmobile users entiality and security characteristic for mobile users.

A. Analysis standard for data security frameworks

via considering the importance of mentioned parameters of MCC, the subsequent analysis parameters are chosen for examination the given security structure the info security frameworks address the protection of mobile user's files formed and manipulation on a portable device or cloud server.

1) Basic theory

The essential structure blocks can be scientific , cryptographic or mathematical standards ,the parameter has been determines fundamental building pieces security systems talked about for MCC. The fundamental hypothesis parameters are incorporated for determination the computational demands of security frameworks

2) *the protection of Data*

The information insurance parameter recognizes the security classification of talked about security systems as ProDCMD or ProDCMC. Various security structures manage information insurance Created and controlled in the cloud (ProDCMC). [13] The the remainder of the security frameworks transact with security systems cover the insurance of Data made and controlled in the device (ProDCMD)

3) Data integrity

versatile clients transfer documents on the cloud server and miss out on physical control of transferred records To overcome the limit of capacity storage of mobile device therefore There must be a system to guarantee the accuracy of clients' transferred documents. The accuracy of the transferred record can be verified with support of integrity verification. The data integrity parameter determine the regard of the integrity verification issue .

4) Scalability

The security system is considered very scalable, wherther the expansion in clients can be consistent overseen without corrupting execution or change in the physical foundation.Scalability is the capacity of the framework to deal with the developing number of clients in an exquisite way. In the event that the proposed security structure is it relies upon a unified server oversaw by an outsider to give security includes, the versatility of the system is assumptions moderate,or else poor.

5) Assumption

the security structure is considered safe werther the implicit considered of the framework are weaker.
for providing security features in an MCC environment. The parameter presumption determine components that are expected to becom (fully trusted , semi-trusted , or distrusted) ; Semi-trust means that several functions are supposed to be completely executed, but some probably traded off,, for exampl storage may be exposed but calculation is appropriately led.

6) the access of Data

if client particiate encrypted files situated on cloud server with gatherings of people and authorized users can access and decrypt file naturally then The access to data in the cloud can be considered as Automated (without the physical support of the file possessor) and if the client needs to use other means such as (email, SMS or call) and send mystery information (for example, a password, secret key) to get unscramble the transferred document and the Access to data is considered semi-automated . .so the Access to data can be spilt in three classes: (a) automated (b) semi-automated (c) manual .

7) Authentication

there must be an a mechanism to check the maker of the file If a mobile client transferred file to the cloud server to share with various clients The validation component can check the creator of file , The authentication variable recognizes the consideration of verification issue

B. Analysis standard for application security framework

For supply better services to users of mobile devices the Application security structures address the security of portable app or mobile app model [14] this one utilizations cloud resources
The chose evaluation parameters are talk underneath:

1) Type of application

app. to recognize the portable App model or kind of mobile app the type parameter has been utilized . which security side are insured in MCC environment.

2) Security features

Security features can be data security, data integrity identities of pravicy , area protecction , authentication, secure management of data access ,hazard administrationor, secure directing.The security lineaments parameter distinguishes the security secured part of portable applications or mobile app. model in the mobile cloud computing environment

3) Assumptions

The system is viewed as sheltered if the basic the suppositions of the administrators are weaker. The supposition parameter distinguishes the parts expected to be totally Trusted , semi-trusted or questioned to give security feature

4) Scalability

if the expansion in clients can be adaptively overseen without debasing execution or change in the physical framework.Seccurity structures proposed for portable applications or the mobile app model are regarded to be so scalable In the event that the proposed security structure is it relies upon a brought together server oversaw by an outsider to give security includes, the versatility of the system is considered moderate,or else poor.

V. SECURITY AND CONFIDENTIAL ISSUE IN MCC

A. Mobile Terminal

The security issues in the portable terminal are quite serious .generally, Just for that the mobile terminal has the accompanying qualities : open working framework; support the third-party software;bolster the outsider programming remote access Internet anyplace and whenever.; "personalization"

1) Malware

Some malware can be download naturally and transported , obscure to the client, with valuable program and frameworks.Therefore the malware gets illicit access to the individual data, even prompt an expansion in execution and automatic payment without any user operation. the client of the portable terminal will sustain from the economic harm or leakage of information For this reason,. the mobile terminal always Get the attention of the attackers because of Openness and its flexibility.
with the increase in the complication of malicious attacks, anti-malware arrangement should provid9e the same action with the one in the desktop processing malware, some security providers have develop anti-virus software for mobile devices. But . Meantime, the portable terminals are limited in abillity and resources which make the antimalware measures that require a meaningful computation resource Hard to accomplish. On the other hand, we should offer answers for recognize and avoid malware in the mobile terminals, which adds to the challenges of doing anticipate malware ,based on the issues the malware can be disseminated among portable terminals in an assortment of structures, for ex, USB interface, 3G system, Bluetooth or MMS connections, . Also, our answers must adjust the rate of location and utilization of assets and software complexity .

2) Software vulnerabilities

a. Application software

Most cell phone clients are accustomed to working the phone through mobile phone administration programming, As now, the cell phone is the principle mobile terminal. which deals with the records on the portable phone over the content synchronization among the telephone and PC. FTP (File Transfer Protocol) by and large applies to this process.
the harm of individual data and unlawful access, intentional removal and a malicious modification can be achived . As we as a whole know because .the username and password of FTP are exchanged to the system and enrolled in design record in specific content. That will make the illicit access a portable device utilizing FTP from PCs in a same net In fact,the attackers can intrude on the portable phone in the error of the app software . the vulnerabilities of the application the software is quite common because the application the software itself is not relatively rigorous

b. Operating system

The working framework is responsible for the administration and control of hardware HD and software SW resource .and becouse it is software very complex that it will exits coding defects , in certain conditions , the errors will be utilized to damage the cell phone by the attackers. these come from programming errors .

3) Other

A security problem in the portable terminal still comes in the form of mobile device customers themselves .In addition, there are many problems in the mobile terminal for security Initially,, mobile users may work incorrectly; secondly, mobile phone customers generally lack security awareness. So we need to identify and anticipate abnormal behavior of customers.

Due to previous problems in the mobile device, attacks can cause loss of privacy, loss of information, and damage to devices across all types of attack ways , as show in Fig 2 .

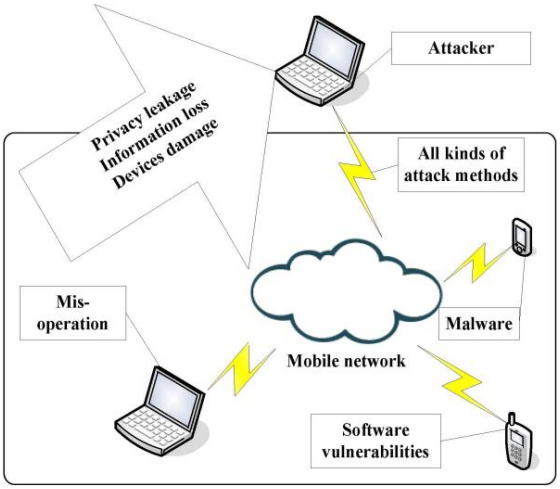

Fig-2: Mobile terminal security issues

B.Mobile net security

the mobile net Expands the net node and user access method due to its mobility and versatility. compare to the traditional network,. the portable devices can access the network in large number ways and The network node extends to the mobile devices that include smartphones, tablets, etc. for example access the network can be , smartphone users can usage the phone services , short message service (SMS) and other web services via 3G network . In addition, most smartphones can also access the network via Wi-Fi and Bluetooth Subsequently, The wide access ways (SMS, Wi-Fi, Bluetooth and so on.) will bring greater security dangers like lthe communication between mobile phones and Mobile cloud sevice providers are also common different interfaces..This will likewise prompt greater security dangers and .lose delicate data or malignant assault For example, different sorts of open spots, (for example, Cafe, eatery and airplane terminal, and so on.) can give Wi-Fi and numerous individuals will open a workstation and access the Internet by free Wi-Fi. For that situation, the potential data the leakage will happen notwithstanding this kind of open Wi-Fi, Even private Wi-Fi additionally faces security dangers, on the grounds that the Wi-Fi encryption system is a shortcoming. Likewise,

C . Mobile cloud

1) Reliability of the platform

the goal of the malicious attacker hacker steals useful information or a valuable services On the one hand and The cloud platform is liable to being attacked due to its high intensity of information resources of users , on the other hand the purpose of the malicious attackers is to deny of service in cloud . For ex Attack denial of service (DOS) will pulldown the platform These attacks can come from the external malicious, legal CC cloud computing IT user, or within the cloud computing staff the operators
availability and close the service in the cloud. will face the risk of data loss When users convey all thier information to cloud service supplier without the definition costly Backup and Disaster recovery service,. In the past years, such events have occurred in cloud suppliers now and Nevertheless. Then, At that point, the cloud supplier must incorporate the present security advancements to give service and clients you ought not depend excessively on the cloud provider.

2) Data protection and confidentiality

To ensure secret information, the single means isn't sufficient We require a total security answer for secure information security and client protection.

in cloud the property and management of the user's data are separate , that makes the worries of the client own information resource becomes the major constrain to the popularization of MCC . Data protection and security are serious problem in the MC . first is place the user data which is randomly stored in the shared infrastructure around the world , and client don't know accurate location in which their data is stored. Then the users Private information faced a greater risk of disclose . [15].

VI. CURRENT PRIVACY AND SECURITY APPROACH TO MCC MOBILE CLOUD COMPUTING

to deal with security and confidentiality of MCC, and more subtle elements on control of portable terminal , net access and transmission security , protection assurance , key administration and encryption , net acess control , and so on.we will look in the current ways

A. aiming security of mobile terminal

1) Anti-malware

we can transfer malware location towared cloud so we can enhance the discovery rate and decrease the consumption of portable terminal resources.For the mobile terminal, there are two activities with the objective in the malware. first one is to detect and eliminate malware.

To cope the restriction of the resources of portable terminal,
While a malware is discover, the legitimate software of cloud can be provision to the portable terminal and executed for eliminate the malware this lawful SW means that it is authenticated and accredited, and can be restored to the portable terminal.
Cloud AV provides several important the benefits are: Cloud AV is an exact instance of anti-malware. better detection of malicious software Cloud AV is a new pattren for detecting malware on mobile devices terminal based on provide an anti-virus like int–cloud net service ; take out the effect of antivirus vulnerabilities;

to greatly improves the detection rate , previously infected hosts review Detecting of it ; improved abilities of forensic ; better administration and improved deploy ability and because it includes two behavior detection engines and the cross - platform host agent & a net services with ten antivirus engines which enormously enhances the discovery rate -[16].
The other is the prevention of malware. the behaviors of users must be careful. To avoid download and installed malware in the mobile devices

2) Software vulnerabilities

For software vulnerabilities, to decrease vulnerabilities of software, We shoud embrace a sequence,of technical measures. For example, integrity of the product is the important policy before applying the product and check the legitimacy and ,the clients should focus on the mobile devices update information , operating system of Phone, and duly download and installation repaire or lates versions of the research and operating system development company. meantime, they should be wary to download the third party software .

3) Regulation of user behavior

Numerous malware are downloaded and executed due to misuse of users or shortage of safety knowledage . So key measure to prevent malware is enhance the safety awareness of the client For example, strange connections don't click ;to receive the data sending from a unknow phone Be careful ; new unauthorized software avoid installing ; turn off the Wi-Fi interface or ,Bluetooth etc. then will be reduced the possibility of transmission of the malware etc.

B.Aiming for (Mobile Network Security)

Now, let's see two aspects of the security in what way to protect the mobile network . One aspect is the data encryption. seeing as only the encrypted information is somewhat secure for the time of the transition via the mobile net, It does not make a difference in what way mobile devices connection the mobile net. The another one is the security protocol(cryptographic protocol or encryption protocol) . For all patterns of arrival way , security protocol search is at the heart of minimize diverse attacks.

C. Aiming to Mobile Cloud Security

1) Platform reliability protection

For both clouds' providers and users, the Reliability and availability of the MCC platform are important. First, cloud provider's current security technologies should be integrated , included VPN technology , verification and entry control, encoding and another technological means and consequently they can give the uninterrupted service available agiest various attacks such as deny of services DOS attack and steal of information. Second, to recover user data when attacks occur the cloud provisioner should offers a full Backup and Recovery solution by these way the cloud platform can increase quality of service (QOS) and increase client trust.

2) Key management & Data encryption

To avoid critical information from seeping out , the Data must be saved in cryptogram text in the cloud confidential data needs encryption technology during the survival period from storage to transmission. , anyway encoding will decrease the usage rate of data, as a result the focus is a transmission to effectively studying and processing the encrypted text. present search on encrypted text process is a confidentiality homomorphism algorithmic program meantime, key management is other significant function for enterprise users.

3) Access control & Authentication

Presently, there are two sorts of validation ways , which draw in huge consideration. One is a client -centric identity authentication . In that way , client is recognized and characterized by identifiers, attributes or characteristics, and client can be permitted for have multiple identifiers. In this approach, you can examine a desired user-centric identity managemen mechanism for MC mobile clouds [17]. The another is behavioral verification in which you can determine clients via their habit & behaviour as remembered Data, their belonging . With this implicit authentication, we can diminish the risk of portable cloud extortion.
At the point when clients finishing transmitting information to the cloud , the AC acc-control will play a direct role . Presently, it exist two types of access control mechanism . One is to assign the entrance authorization for a level of record, and every one of the occupants shared this designated account . another is to pre-assign the entrance authorizations for the related inhabitant accounts utilizing the mechanism of the entrance control list (ACL) [18].

4) Protection of privacy

Up to this point, to shield the confidentiality of data, the governments from everywhere throughout the world have officially built up the assurancce design and system. For ex, the government of British presented the Data Protection Act in 1998 , and The European Union has distributed EU information security mandate in 1995, et cetera Then again, modernization strategies have constantly assumed an essential part in security insurance P3P (Platform for Privacy Preferences) is an extremely illustration, declared by the WWW consortium an electronic agreement on the protection of privacy of protection of individual information among the net service providers. Presently , 40 % of the main 100 worldwide pages are utilized or intend to utilize P3P innovation it is also encourage by a few researchers
In summary, in table 1 introduced current ways to deal with security & the privacy of MCC
.

Security issues		Current approaches
Mobile terminal	Malware software	Detection and prevention CloudAV
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others(lack of security awareness, mis-operation)	Regulating the users' behavior
Mobile network	Information leakage or Malicious attack	Data encryption
		Security protocol
Mobile cloud	Platform reliability	Integrating the current security technologies; Key management and data encryption; Authentication and access control Privacy and data protection
	Data and privacy protection	

Table I. Security issues and current Corresponding approaches

VII. CONCLUSION

-In this paper, we present a comprehensive survey of security and privacy challenges, and their security solutions of MCC. Firstly, we provide a background overview of MCC. Then, we discuss the potential security and privacy challenges of MCC.

so that the readers in this field can compare, analyze and direct further research activities. However, although this research field is still immature and unexplored in depth, many security and privacy related challenges are still under research, and yet to be solved. Hence, finally, we d summarize some Security issues and current Corresponding approaches in table 1 . We hope that this paper will be beneficial in giving a hint the way ahead, and enable a massive integration of mobile computing and cloud computing

REFERENCES

[1] P. Cation, "cloud Comput ting Securit ty Issuues - Challen nges a Opporttunitie s," pp. 33–42, 2017.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[3] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," *MIPRO, 2010 Proc. 33rd Int. Conv.*, pp. 344–349, 2010.

[4] H. Nicanfar *et al.*, "State-of-The-Art of cloud computing cyber-security," *Proc. 2015 IEEE World Conf. Complex Syst. WCCS 2015*, vol. 3, no. 4, pp. 0–176, 2016.

[5] E. G. Report, "The future of cloud computing," *Analysis*, vol. 1, no. 1, pp. 1–26, 2010.

[6] A. Buczkowski, "Location-based Marketing: the academic framework," p. 58, 2012.

[7] A. Shahzad and M. Hussain, "Security Issues and Challenges of Mobile Cloud Computing," *Int. J. Grid Distrib. Comput.*, vol. 6, no. 6, pp. 37–50, 2013.

[8] D. Hutter, "InfoSec Reading Room Physical Security and Why It Is Important," 2013.

[9] W. Song and X. Su, "Review of Mobile cloud computing 1) Hardware of handheld equipment and independence Virtual layer," *City*, pp. 1–4, 2011.

[10] H.T. Dinh, C. Lee, D. Niyato, P. Wang, A survey of *mobile cloud computing: architecture, applications, and approaches*, Wireless Communication and Mobile Computing. http://dx.doi.org/10.1002/wcm.1203

[11] D. Kovachev, Y. Cao, R. Klamma, *Mobile cloud computing: a comparison of application models,* computing Research Repository, CoRR, vol. abs/1009.3088,2010.

[12] L. Guan, X. Ke, M. Song, J. Song, *A survey of research on mobile cloud computing,* in: Proc. 10th IEEE/ACIS International Conference on Computer and Information Science, ICIS '11, Sanya, China, Nov. 2011.

[13] L. Dupré and T. Haeberlen, "About ENISA Legal notice," no. December, 2009.

[14] H. Qi *et al.*, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 1, no. 1. pp. 1587–1611, 2014.

[15] L. Guan, X. Ke, M. Song, and J. Song, "A survey of research on mobile cloud computing," *Proc. - 2011 10th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2011*, pp. 387–392, 2011.

[16] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," *Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW '09*, p. 127, 2009.

[17] X. Wang, M. Chen, T. T. Kwon, L. Yang, and V. C. M. Leung, "AMES-cloud: A framework of adaptive mobile video streaming and efficient social video sharing in the clouds," *IEEE Trans. Multimed.*, vol. 15, no. 4, pp. 811–820, 2013.

[18] D.-G. FENG, M. ZHANG, Y. ZHANG, and Z. XU, "Study on Cloud Computing Security," *J. Softw.*, vol. 22, no. 1, pp. 71–83, 2011.