Data Security Issues in the Realm of Mobile Cloud Computing : A Survey

Mohammed-Ali Anwar
Manchester Metropolitan University, Manchester, UK
mohammed-ali.anwar@stu.mmu.ac.uk

Abstract

Mobile Cloud Computing (MCC) is a recent technological development, which has emerged from two popular technology trends; mobile computing and cloud. In essence it revolutionises the capabilities of mobile devices by integrating both storage and processing of the cloud environment with mobile computing and in doing so providing greater optimisation and operating power, allowing for transparent and seamless use of resources provided by the cloud. However, expanding the capability of resource constrained mobile devices in this manner comes at a price. There are many risks associated with the security of data within the cloud environment and as MCC essentially uses the cloud, it also inherits any security issues that are associated with cloud computing. The aim of this survey is to identify potential data security issues, and analyse and present some pioneering security mechanisms and finally suggest some future directions for better data security with MCC.

Keywords: Data security, mobile cloud computing, data integrity, privacy.

1 Introduction

Each and every day millions of people around the world are using hand-held "mobile' devices (i.e. Smartphones, PDAs and Tablets) in order to run software applications which (securely) provide them with access to important information, such as; the people, locations, products and services available around them [1, 2, 3, 4]. These software applications also provide users with a method to interact with people that they may do business with or with whom they associate. The technology used to make all of this possible is known as Mobile Cloud Computing or MCC.

MCC essentially brings new and exciting applications to mobile devices beyond what could have been possible by regular Mobile Computing (MC) applications, all done by combining both cloud computing and mobile computing technologies [5, 6, 7, 8]. By combining both CC (Cloud Computing) with MC a new infrastructure has been invented which relieves the stress off of mobile devices from requiring huge amount of processing power as well as storage, as

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

the storage and 'heavy lifting' of computing intensive work is now taken over by the cloud [8], which resides outside of the mobile computing ecosystem. In short Cloud Computing offers various services (e.g. IAAS, PAAS and SAAS) to Mobile Computing as a means to tackle the issue of lack of storage space and processing power most mobile devices offer; which have a tremendous impact on service quality [9].

Currently, MCC is a very hot topic of discussion in the technology world as well as in academia [10]. The IT industry highly anticipates that Mobile Cloud Computing will have a drastic effect on people's life styles and work patterns in a future networked world [11]. IBM predicted that there will be "1 trillion cloud-ready devices by 2015" and stated that users of MCC will primarily work using web-based applications via remote servers which are accessed through networked devices [12, 11, 13, 14, 15]. Although Mobile Cloud Computing may seem like an amazing technological advancement which all individuals and businesses should be taking advantage of. There still remains a lot of mystery around the subject as well; more specifically around Data Security surrounding where highly confidential business data would be stored, as well as how the data will be transmitted securely and reliably between cloud service users and the cloud, etc.

This paper is organised as follows. Section 1 is an introduction to the paper. Section 2 provides an overview of MCC and the paper, and the advantages and motivations behind MCC as well as the applications of the technology. Section 3 discusses MC (Mobile Computing) and CC (Cloud Computing) in MCC. Section 4 discuses data security implications of MCC, Section 5 describes some of the main issues and security mechanisms in Data Security for MCC, Section 6 research opportunities and future technology challenges to better secure data in MCC. Section 7 concludes the paper.

2 MCC an Overview

According to Din. 2013 in [16] the term Mobile Cloud Computing (MCC) was introduced to the world not long after the concept of Cloud Computing. It is a technology that is not only attracting the attention of everyday consumers but is also attracting the attention of many entrepreneurs as a profitable option for business use, as it substantially reduces the running and development cost of MC applications, as well as providing a richer experience of mobile services at a low cost.

To understand what mobile cloud computing is; it is first necessary to understand what cloud computing is [17]. This paper provides information about what cloud computing is, the different services provided in the cloud, security and privacy issues surrounding mobile cloud computing, and surveys the various types of data security mechanisms which have been proposed by experts in the field of computer science and cloud computing. The paper also presents a comparative analysis of research around the area of Mobile Cloud Computing (MCC), as well as future directions for better security of data within mobile

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

Table 1: Advantages and motivations for MCC

Approach	Advantages/ Benefits of MCC	Motivations for MCC
[10]	Intelligent Balance load; Convenient access to data on-demand self-service; Breaking through the hardware limits	Extended Battery power due to processing done via the cloud and the mobile device being used as a thin client.
[18]	Converting mobile devices in to virtual, personal & portable desktops; Increasing battery life & computing power of mobile devices; Off-loading unlimited mobile connectivity to emergent mobile cloud infrastructures; Increasing resource sharing; Reduces costs of mobile-based application development	Addressing the issue of battery life & processing power of MC; Coping with the increasing needs of mobile users, with low-end devices; Eliminate current limitations of MC
[19]	Improving reliability; Dynamic provisioning; Scalability; Multi-tenancy; Ease of integration	For the means of on-demand self-service and extendibility, it offers the infrastructure, platform and software services in a cloud environment to mobile users through mobile network.
[20]	Long battery output time; Enhanced processing power and data storage space; Extended processing power and data storage; Extra data and application reliability; Scalability; Multi-tenancy; Flexible Integration	Offers users software applications, processing and storage capabilities of the cloud without having to invest on the infrastructure.

cloud computing.

This section provides information about the advantages of MCC technology as well as the motivations and some of its main applications.

2.1 Advantages and Motivations for MCC

2.2 Applications of Mobile Cloud Computing

To understand the importance of the security and privacy of Mobile Cloud Computing it can be very useful to know some of its applications first [21, 22, 23, 24]. Over the years users of MCC have witnessed the release of several applications for mobile devices. Including but not limited to: M-commerce, Multimedia-sharing, M-sensing, M-learning, M-healthcare, M-gaming, Location-based mo-

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

bile services and even Augmented Reality [5, 25].

Below is a description of some of the most commonly used applications in MCC [18]:

Mobile Commerce (m-commerce)

Mobile commerce is becoming a really popular trend with businesses as almost everyone has a mobile device. M-commerce can be put in to a few categories of applications, including but not limited to; education [26], finance, advertising and shopping [18]. As stated by [20, 27] MCC provided a solution to the world of commerce by making it easy mobile users with low bandwidth, storage power and battery life by making use of the cloud environment.

Mobile Learning (m-learning)

Mobile learning is essentially e-learning services that are catered towards mobile devices generally with the aid of mobile cloud computing services. Traditional mobile learning applications have a few limitations which include, a huge cost in mobile devices and network, lower network transmission rate, and somewhat limited educational resources. However, since the invention of mobile cloud computing, these are no longer really an issue [18]. As stated by [20] using MCC provides e-learning resources with large storage space and high processing capabilities, which also introduces the idea of cloud-based m-learning eliminating the current barriers of the technology.

Mobile Healthcare (m-healthcare)

Mobile healthcare has revolutionised the healthcare industry in that it offers healthcare professionals working in hospitals and healthcare organisations the ability to access a variety of on-demand services on clouds rather than owning standalone applications on local servers. This will not only cut costs but will also allow for much more flexibility in accessing resources [28, 18]. M-healthcare in MCC eliminates the issues surrounding classical medical applications used for medical treatment. Allowing m-healthcare users access medical resources in an efficient method utilizing the availability of on-demand services provided by the cloud [20].

Mobile Gaming (m-gaming)

Many industries have been taking advantage of mobile cloud computing technology. These industries include; the gaming, healthcare, and education industries. Mobile gaming can now off-load computational power to the cloud [18], meaning users no longer need powerful devices to be able to run games and can essentially just use the mobile device as a thin-client with the computation and graphics rendering done entirely via the cloud [9, 20].

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

3 CLOUD COMPUTING & MOBILE CLOUD COMPUTING (MCC)

A large amount of technology consumers across the globe are using a variety of different computing devices, (i.e. tablets, laptops, smart phones, etc), they are not only using these devices at home but are also increasingly using them in the workplace as well as when in commute. This is causing an increasing demand in IT to deliver its services in a unique manner that will allow the services to be used across a variety of devices and operating system platforms (i.e. Microsoft Windows, Linux, Mac OS, etc.) seamlessly. The information Technology community has resolved this issue by releasing a new service delivery mechanism known as Cloud Computing [29].

Living in today's largely interconnected world, surrounded by advanced and ever affordable technology and where almost everyone has access to the Internet, mobile cloud computing has unquestionably become a very hot topic of discussion among the technology community. As stated by [28] This technology has primarily been introduced as a means to 'set-free' individual devices from requiring to possess large processing or storage capacities, instead these requirements could be transferred to the cloud. Therefore, cloud computing can be thought about in a few different ways; from providing remote data storage to the complex structure enabling fully-fledged platforms of services according to individual's personal requirements.

Mobile cloud computing has tremendously evolved in recent years, as stated by [28], this is "mostly due to the expansion of the smart phone market". MCC in its simplest is an infrastructure where both the storage of data as well as the processing take place outside of the mobile ecosystem [16]. MCC often involves three technology foundations, namely; Mobile Computing (MCC), Cloud Computing (CC) and Computer Networks [18].

4 DATA SECURITY IMPLICATIONS OF MCC

According to a survey mentioned by Khan, et al. in [17] 74% of IT executives and Chief information officers are not accepting using cloud services due to there being a high risk with data security and privacy with using the technology.

In the research conducted by Kumar and Lu in [30], they suggest that the data security settings rely on the IT management that the cloud provides to the mobile device. A security issue such as a 'bug or security loophole' could result in a data security breach. A good example provided in [31] is a bug in Google which appeared in 2009 causing a number of sensitive user documents to be shared without the owner's consent or knowledge.

Data and information that is stored on the cloud can at often times be seen as valuable to individuals with malicious intent. Every day there are thousands of individuals that are storing sensitive information or potentially sensitive data on their computers, and this same information and data is being transferred and stored in the cloud; either for easy accessibility or for security reasons. This

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

makes it crucial for individuals to understand the security mechanisms that the cloud provider has implemented and it is equally important that individuals also take precautions to secure their data as well, this includes securing mobile devices themselves, as they are also susceptible to malware at stated by Mollah, Azad and Vasilakos in [32].

Before talking about data security issues and mechanisms to protect data in mobile cloud computing, it is important for us to understand that any security issues that are present in cloud computing will also inherently be present in mobile cloud computing. By definition, mobile cloud computing is essentially connecting mobile devices to a remote cloud. The remote cloud is essentially the same as a conventional cloud services provider. This makes general cloud computing threats applicable to mobile cloud computing as well [33].

5 Data Security Issues and Mechanisms in MCC

5.1 State risk within MCC

When it comes to securing user data within the realm of Mobile Cloud Computing (MCC) it is important to be informed of the different states data can occur and the controls that we have at hand for when in that particular state. With the rapid increase in the use of Mobile Cloud Computing over recent years, protecting 'data-at-rest' is now considered to be equally as important as protecting data when in transit [34].

- Data-in-rest: This is essentially data which is 'inactive', that is physically stored on NAS, SAN, file servers taking the shape of 'databases, data warehouses, off-site backups, etc'. As well as encryption, strong access control policies and data virtualisation need to be administered to prevent attacks.
- Data-in-use: This is essentially the dynamic data that is stored in non-persistent state, this could include:
  - Data or encryption keys stored in cache
  - Main memory
  - Data that is currently being processed by an application
  - Transactions that are in a message queue

Issue with data-in-use in MCC

Data like this is generally stored in a cleartext form, as it is used for conducting 'value-added' functions, i.e. Searching. It is now recommended by the Data Security Alliance to encrypt data that is in the data-in-use state for more security.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

Solution for data-in-use in MCC

Complete homomorphic encryption enables computations on encrypted data/ or ciphertext, when this is performed, results that are obtained when decrypted will match computations that are done using plaintext [35].“Enclaves are used to secure data-in-use in which data are in encrypted form in RAM but available as clear text inside CPU” [34].

6 Data integrity attacks

Data integrity risk

Data integrity is crucial when talking about MCC security as if the data is not as expected after transmission or storage on the cloud it could have huge security implications for a company which deals with a lot of sensitive data.

As stated in [28] data integrity is crucial when talking about MCC security as the data storage and processing take place on the cloud service provider's end, outside of the mobile computing ecosystem. Here data integrity is of up most importance, more specifically the accuracy and consistency of the users' data. Integrity is important as it prevents undetected modification of data from occurring, whether it is from unauthorised users or systems. The violation of the integrity of data can have a tremendous effect on mobile users and could mean business loss, economic loss as well as other devastating losses to the user.

Possible Security Mechanism

A traditional solution to data integrity is to essentially store encrypted data on the remote server. In comparison with a desktop computer, it is not feasible to encrypt data before uploading the data to the cloud; this is due to the cost in computation for running the encryption algorithm [5]. In [36] Dijk, et al., have developed a protocol to essentially encrypt and store data in the cloud.

This works by having the encryption key initially stored on the cloud via the user, then the user will upload the plaintext to the cloud for encryption. The data is then divided into blocks of equal length, each of which are encrypted utilizing the previously uploaded encryption key. After this procedure an image is created from each of the encrypted blocks.

Testing data integrity after encryption

A block can randomly be selected, then a request can be sent to the cloud server to fetch the image of the data block which the user has requested within a *timeout interval and if the resulting returned image of the data block matches up with that of the one which was locally computed by the users mobile device. Then the user can consider it as the data having been encrypted correctly.

*Timeout interval (above). This is the maximum time required by the cloud server to transfer the requested image of the data block back to the user, which is typically smaller than the amount of time required in the process of encrypting

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

the data block, selected afresh and generating an image from the encrypted data block. However, there are also certain factors that have to be taken into consideration, i.e. a limited wireless bandwidth that may affect the transmission time [5].

The other of [5, 36] state that a mobile client must also ensure that the application code running on the cloud is indeed the same application code it authorises the cloud to run (called code integrity). There seems to be very little research conducted in the literature regarding the code integrity. It is crucial to make certain the correctness of application execution especially when dealing with computation/ code offloading, code integrity is key and as stated in [37] "loss of integrity can leads to modification attack".

7 Service Availability, Security Risks and Mechanisms

Service availability risk

Availability and reliability of MCC is crucial both for the user as well as the cloud service provider, this could be a security issue as stated in [37] by Bhatia and Verma, availability ensures that authorised parties are able to access information when required.

[37] Denying access to information for example, leads to denial of service attack in which even legitimate users are denied access to resources on the server.

Both [9, 38] state that availability of data is more of an important issue within the realm of Mobile Cloud Computing than it is in wired networks when dealing with Cloud Computing. Users that are using 'mobile' hand held devices may not be able to access the cloud to obtain a service due to factors like traffic congestion, network failure, and the out of signal issue.

Possible Security Mechanism

Both [39] and [40] provide possible mechanisms that can overcome the availability issue in MCC in the specific issue of disconnection from clouds. [39] Provides details of a discovery mechanism that searches for local nodes in the current location of the MCC user whose current connection to the cloud is not available. After detecting the presence of existing near-by nodes that are currently in a stable mode, the target for the application is essentially changed. As opposed to having a connection/ link directly to the cloud, an MCC user can establish a connection to the cloud using neighbouring nodes in an adhoc method. This technique however does not take in to account things like; mobility, privacy of neighbouring nodes or the capabilities of the devices used.

Another possible mechanism which resolves the issues of the above mechanism is provided by [40] and also stated in [9]. Suggests a WIFI based multi-hop

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

networking system known as 'MoNet' as well as a distributed content sharing protocol for the issue as well as without any infrastructure.

As opposed to the solution provided by [39] this mechanism also takes in to account mobility and moving nodes in the users current location. It works by having each node broadcast messages periodically in order to inform other nodes of its status (i.e. systems parameters and connectivity) as well as local content updates. Stated in the messages, each node keeps and maintains a neighbouring node list as well as a content list. It estimates role levels of other nodes based on things like the disk space, power supply and bandwidth. The nodes with the shortest hop-length path as well as the largest role level are chosen as the intermediate nodes to receive content.

Other security issues are also taken in to consideration by the authors of the above mechanisms, i.e. they take care of security issue for mobile clients when they share data by using an account key, a friend key and a content key. The first to authenticate and encrypt the data, the second to secure the channel between two reliable users and the third to protect access control [39].

7.1 Multiple Locations for Storage and Computation

7.1.1 Risk of data stored and processed in multiple locations

Gu and Guirguis in [41] state that data that is stored on hand held mobile devices is often transferred and stored in the cloud. As well as this, it is extensively off-loaded and executed in the cloud and in turn making the data and code vulnerable to attacks at multiple locations. For example, any user data will now be vulnerable in the mobile device [41, 32] itself as well as, the cloudlet and the cloud. The links that were used in uploading the data and code could also now be susceptible to attack.

In short, attackers have the option of targeting the weakest resource available in the 'chain' to gain access to sensitive information as well as have the ability to compromise the integrity of the computation. The involvement of third parties when utilising cloud computing with mobile further complicates the issue at hand. In the following, we review some of the possible security mechanisms

As stated by Suo, et al. in [10] any sensitive data used in transmission or storage in MCC to the cloud needs to be in cipher form to prevent it from being leaked. However, this will also decrease the utilization rate of the data, therefore attention will be given to efficiently analysing and processing the cipher text. In [35] and [10] the authors have taken this issue in to consideration and have pointed out current research that is taking place on the homomorphic algorithm, which essentially enables computation being made on encrypted data or cipher text. Key management also needs to be taken into consideration when talking about data encryption [10]. Other security mechanisms include protecting access to the data with use of Authentication and Access Control and the security in the privacy of data when stored in the cloud.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

7.2 Additional data security mechanisms under research for MCC

8 Research Opportunities and Future Challenges

In this section we are looking at future opportunities and directions to better secure data within Mobile Cloud Computing.

8.1 Biometric Encryption in MCC

The idea of using Biometric Encryption in protecting user data in Mobile Cloud Computing is something to take in to consideration in future opportunities as biometric technology is considered to be quite secure and we have been utilising this technology already in Mobile Computing (MC) and in many other applications. However, as MCC is a combination of MC and CC, implementing this technology can be challenging.

Zhao et al., in [47] have conducted an examination of the various aspects of using Biometric Encryption (BE) within the MCC environment in an effort to solve data security issues. They address the problem area of using BE in MCC, as well as propose an advanced protocol utilizing BE for transmitting private data in an MCC environment, along with designing a conceptual cloud platform enabling authentication with the use of biometric technology to serve as a data centre in the future.

8.2 Mobile Cyber Security in MCC

This is a huge topic which is currently under research in academia as well as in industry, as stated by Chang, et al. in [18] Security of every level of MCC needs to be taken under consideration, including; mobile cloud infrastructures, networks, platforms and service applications. Typical topics which need to be given attention to include [18]:

- Mobile data and information security
- End-to-end mobile transactions
- Secured mobile connectivity,
- and Security management and assurance on mobile clouds.

9 Conclusion

As technology, more specifically mobile devices continue to evolve, mobile cloud computing is definitely the present and foreseeable future of the IT industry [48, 49] and will remain a very hot topic in the research realm for some time to come. Mobile cloud computing provides fantastic benefits to its users (not to mention cloud service providers). Currently, people that are looking for mobile cloud

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

Table 2: Data security mechanisms under research for MCC

Approach	Proposed Mechanism	Mechanism Type	Advantages/ Drawbacks
[42]	Confidentiality and Access Control with HIBE	(HIBE) Multi-level hierarchical identity-based encryption	Highly efficient, has low overhead and highly scalable; Does not take into consideration privacy and synchronization.
[43]	BSS: Block-based sharing scheme	Block based cryptographic system	Support data confidentiality and integrity; highly scalable; Reduces resource utilization, improves response time and provides better security to MCC users
[44]	Homomorphic encryption for data storage and sharing	Homomorphic encryption	Not scalable
[45, 37]	Mobile healthcare on a secured hybrid cloud	Role-based access technique, Crypto-processors, IBE	Computationally intensive
[46]	Secure real-time video sharing and searching in MCC	Uses advanced encryption standard, Searchable symmetric encryption, Digital Signature and Ciphertext-policy Attribute-based encryption.	Highly scalable

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

computing services need to take in to consideration the security implications that may come with using this technology as well as the security mechanisms mobile cloud computing service providers are implementing to find out which best suits their needs.

This survey paper has provided an insight in to the complexity of modern day Mobile Cloud Computing technology and has investigated the most challenging data security issues and presented and analysed the most significant mechanisms to solve these issues. It has also contrasted and compared the solutions provided by different authors against a well-defined criteria.

In conclusion although there have been efforts to overcome the data security issues in MCC, there are still future works in progress, including the ones mentioned in my survey. For example, Biometric Encryption and Mobile Cyber Security in MCC, which could be one of the technologies used in the future to better secure data in MCC.

10 Acknowledgement

I would like my supervisor Dr Mohammad Hammoudeh for the advice he has provided throughout this work.

References

[1] M. Hammoudeh and T. A. Alsboui, "Building programming abstractions for wireless sensor networks using watershed segmentation," in *Smart Spaces and Next Generation Wired/Wireless Networking*, pp. 587–597, Springer, Berlin, Heidelberg, 2011.

[2] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot," *Computer Networks*, vol. 133, pp. 141–156, 2018.

[3] M. Hammoudeh, "Modelling clustering of sensor networks with synchronised hyperedge replacement," in *International Conference on Graph Transformation*, pp. 490–492, Springer, Berlin, Heidelberg, 2008.

[4] M. Hammoudeh, J. Shuttleworth, R. Newman, and S. Mount, "Experimental applications of hierarchical mapping services in wireless sensor networks," in *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pp. 36–43, IEEE, 2008.

[5] A. Aloraini and M. Hammoudeh, "A survey on data confidentiality and privacy in cloud computing," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, (New York, NY, USA), pp. 10:1–10:7, ACM, 2017.

[6] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Constant-size threshold attribute based signcryption for cloud applications," in *SECRYPT 2017: 14th International Conference on Security and Cryptography*, vol. 6, pp. 212–225, Scitepress, 2017.

[7] P. Dibb and M. Hammoudeh, "Forensic data recovery from android os devices: an open source toolkit," in *Intelligence and Security Informatics Conference (EISIC), 2013 European*, pp. 226–226, IEEE, 2013.

[8] J. K. Mohsin, L. Han, M. Hammoudeh, and R. Hegarty, "Two factor vs multi-factor, an authentication battle in mobile cloud computing environments," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, (New York, NY, USA), pp. 39:1–39:10, ACM, 2017.

[9] A. Carlin, M. Hammoudeh, and O. Aldabbas, "Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 6, 2015.

[10] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, pp. 655–659, IEEE, 2013.

[11] M. Hammoudeh, S. Mount, O. Aldabbas, and M. Stanton, "Clinic: A service oriented approach for fault tolerance in wireless sensor networks," in *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pp. 625–631, IEEE, 2010.

[12] G. C. Deka, *Handbook of Research on Securing Cloud-Based Databases with Biometric Applications*. IGI Global, 2014.

[13] S. Belguith, N. Kaaniche, A. Jemai, M. Laurent, and R. Attia, "Pabac: a privacy preserving attribute based framework for fine grained access control in clouds," in *SECRYPT 2016: 13th International Conference on Security and Cryptography*, vol. 4, pp. 133–146, Scitepress, 2016.

[14] A. Benzerbadj, B. Kechar, A. Bounceur, and M. Hammoudeh, "Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links," *Journal of Network and Computer Applications*, vol. 112, pp. 41–52, 2018.

[15] M. Hammoudeh and M. Arioua, "Sensors and actuators in smart cities," 2018.

[16] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless communications and mobile computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

[17] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 5, pp. 1278–1299, 2013.

[18] J. Gao, V. Gruhn, J. He, G. Roussos, W.-T. Tsai, *et al.*, "Mobile cloud computing research-issues, challenges and needs," in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, pp. 442–453, IEEE, 2013.

[19] D. M. Tank, "Security and privacy issues, solutions, and tools for mcc," in *Identity Theft: Breakthroughs in Research and Practice*, pp. 79–99, IGI Global, 2017.

[20] A. Shahzad and M. Hussain, "Security issues and challenges of mobile cloud computing," *International Journal of Grid and Distributed Computing*, vol. 6, no. 6, pp. 37–50, 2013.

[21] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, "Security threats to critical infrastructure: the human factor," *The Journal of Supercomputing*, pp. 1–17, 2018.

[22] I. GHAFIR, V. PRENOSIL, M. HAMMOUDEH, T. BAKER, S. JABBAR, S. KHALID, and S. JAF, "Botdet: A system for real time botnet command and control traffic detection," *IEEE Access*, 2018.

[23] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," *IEEE Access*, vol. 6, pp. 25167–25177, 2018.

[24] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in *Computer and network security essentials*, pp. 603–618, Springer, Cham, 2018.

[25] K. G. Holmes, A. Coates, and M. Hammoudeh, "Motion capture using the internet of things technology: A tutorial," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, p. 40, ACM, 2017.

[26] M. Farhan, S. Jabbar, M. Aslam, M. Hammoudeh, M. Ahmad, S. Khalid, M. Khan, and K. Han, "Iot-based students interaction framework using attention-scoring assessment in elearning," *Future Generation Computer Systems*, vol. 79, pp. 909–919, 2018.

[27] R. Newman, M. Hammoudeh, and P. from Heaven, "A retrospective on the use of wireless sensor networks for planetary exploration", ahs," 2008.

[28] S. L. Albuquerque and P. R. Gondim, "Security in cloud-computing-based mobile health," *It Professional*, vol. 18, no. 3, pp. 37–44, 2016.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

[29] A. Finn, H. Vredevoort, P. Lownds, and D. Flynn, *Microsoft private cloud computing*. John Wiley & Sons, 2012.

[30] K. Kumar and Y.-H. Lu, "Cloud computing for mobile users: Can offloading computation save energy?," *Computer*, vol. 43, no. 4, pp. 51–56, 2010.

[31] J. Kincaid, "Google privacy blunder shares your docs without permission," *TechCrunch, March*, 2009.

[32] S. Moffat, M. Hammoudeh, and R. Hegarty, "A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, p. 34, ACM, 2017.

[33] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future generation computer systems*, vol. 29, no. 1, pp. 84–106, 2013.

[34] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, p. 8, ACM, 2017.

[35] I. Mouhib, K. Zine-Dine, *et al.*, "Encryption as a service for securing data in mobile cloud computing," in *Intelligent Systems Design and Applications (ISDA), 2015 15th International Conference on*, pp. 546–550, IEEE, 2015.

[36] M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, "Hourglass schemes: How to prove that cloud files are encrypted," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, (New York, NY, USA), pp. 265–280, ACM, 2012.

[37] A. Carlin, M. Hammoudeh, and O. Aldabbas, "Defence for distributed denial of service attacks in cloud computing," *Procedia computer science*, vol. 73, pp. 490–497, 2015.

[38] A. Huth and J. Cebula, "The basics of cloud computing. united states computer emergency readiness team," *Retrieved July*, vol. 12, no. 2013, pp. 800–145, 2011.

[39] G. Huerta-Canepa and D. Lee, "A virtual cloud computing provider for mobile devices," in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, p. 6, ACM, 2010.

[40] L. Zhang, X. Ding, Z. Wan, M. Gu, and X.-Y. Li, "Wiface: a secure geosocial networking system using wifi-based multi-hop manet," in *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, p. 3, ACM, 2010.

[41] L. A. Holt and M. Hammoudeh, "Cloud forensics: A technical approach to virtual machine acquisition," in *Intelligence and Security Informatics Conference (EISIC), 2013 European*, pp. 227–227, IEEE, 2013.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018

[42] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, "Seco: Secure and scalable data collaboration services in cloud computing," *computers & security*, vol. 50, pp. 91–105, 2015.

[43] A. N. Khan, M. M. Kiah, M. Ali, S. A. Madani, S. Shamshirband, *et al.*, "Bss: block-based sharing scheme for secure data storage services in mobile cloud environment," *The Journal of Supercomputing*, vol. 70, no. 2, pp. 946–976, 2014.

[44] M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," in *Information Networking (ICOIN), 2015 International Conference on*, pp. 493–497, IEEE, 2015.

[45] K. A. Nagaty, "Mobile health care on a secured hybrid cloud," *J Sel Areas Health Inform*, vol. 4, no. 2, pp. 1–9, 2014.

[46] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Network*, vol. 29, no. 2, pp. 46–50, 2015.

[47] K. Zhao, H. Jin, D. Zou, G. Chen, and W. Dai, "Feasibility of deploying biometric encryption in mobile cloud computing," in *ChinaGrid Annual Conference (ChinaGrid), 2013 8th*, pp. 28–33, IEEE, 2013.

[48] E. Mokrov, A. Ponomarenko-Timofeev, I. Gudkova, P. Masek, J. Hosek, S. Andreev, Y. Koucheryavy, and Y. Gaidamaka, "Modeling transmit power reduction for a typical cell with licensed shared access capabilities," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, p. 5505, 2018.

[49] A. A. Ateya, A. Muthanna, I. Gudkova, A. Abuarqoub, A. Vybornova, and A. Koucheryavy, "Development of intelligent core network for tactile internet and future smart systems," *Journal of Sensor and Actuator Networks*, vol. 7, no. 1, p. 1, 2018.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27050v1 | CC BY 4.0 Open Access | rec: 24 Jul 2018, publ: 24 Jul 2018