MOBILE DATA SECURITY: A REVIEW OF LITERATURE

By (Name)

Course name

Professor’s name

Institution (university)

Date submitted

Table of Contents

[List of tables 2](#_Toc524044384)

[Literature Review 3](#_Toc524044385)

[1.1 Broad Scan 4](#_Toc524044386)

[1.1.1 Research journal 5](#_Toc524044387)

[1.1.2 Filing system 6](#_Toc524044388)

[1.1.3 Bibliographic list from broad scan 6](#_Toc524044389)

[1.2 Focused Review 9](#_Toc524044390)

[1.2.1 Updated filing system 9](#_Toc524044391)

[1.2.2 Updated bibliography list from focused review 10](#_Toc524044392)

[1.3 Mobile data security and vulnerability 11](#_Toc524044393)

[1.3.1 Background of the research 11](#_Toc524044394)

[1.3.2 Framework and methodology 12](#_Toc524044395)

[1.3.3 Proposed solution 13](#_Toc524044396)

[1.3.4 Discussion 13](#_Toc524044397)

[1.4 Cryptographic Approach to Mobile Data Security 14](#_Toc524044398)

[1.4.1 Background 14](#_Toc524044399)

[1.4.2 Cryptographic approach 15](#_Toc524044400)

[1.4.3 Proposed Hybrid Approach 15](#_Toc524044401)

[1.4.4 Discussion and conclusion 16](#_Toc524044402)

[1.5 Final Outline of the Literature Review Chapter 16](#_Toc524044403)

[1.6 Introduction 17](#_Toc524044404)

[List of references 18](#_Toc524044405)

# List of tables

Table 1.1 research journal…………………………………………………………………………5

Table 1.2: the filing system from broad scan……………………………………………………..6

Table 1.3: the updated filing system from focused review……………………………………….9

# Literature Review

The work herein is a review of literature on the topic, “mobile data security” as identified and approved in the previous assignment about introduction to research. The task in this assignment will be to conduct a review of previous research on the general topic about mobile data security. The review will be based on two research papers whose basis is mobile data security. The two research papers that will be chosen have a differentiated approach to the topic. The first paper that this work will review takes a contemporary approach to the topic and bases its discussion on mobile security as the protection of such devices and in particular the vulnerability of smart phones to attacks (Samaher 2016, p. 3-10).

The second paper that this assignment will conduct a review on takes a cryptographic (technological) approach to the problem, and provides a rather unique solution, the use of cloud computing to enhance the security of mobile data in the wake of increased vulnerability of such devices in the physical care of owners (Sujithra, Padmavathi & Narayanan 2015, p.480-485).

However, the review of the two papers will be a step-by-step approach as follows: Section 1.1 comprised of a broad scan of the topic outlining the research for those papers to be considered for review, a collection of such papers and a bibliography of those papers considered. Right after that was section 1.2 in which this work narrowed the research scope to come up with a focused scan of all those papers relevant to the topic. This involved filtering out those papers whose scope is relatively irrelevant to the problem at hand; this also included updating the bibliography field to only include those papers that made it to the focused scan section. Next were sections 1.3 and 1.4 in which this research conducted the review of the two selected papers. Sections 1.5 and 1.6 comprised of the final outline of the review of literature while is an introduction to the same.

## 1.1 Broad Scan

While conducting the search, this section involved carrying out a broad scan after identifying and selecting the topic to do a literature review on. The search involved the use of the keywords to look up the research papers on different platforms on the internet, mainly Google Scholar, Research Gate and IEEE Xplore digital library. After the search, the resultant papers, fifteen in number, were selected and included in the bibliographic field.

### 1.1.1 Research journal

*Table 1.1 research journal*

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Task** | **Action** | **Comment** |
| 20/08/2018 | Queried the internet for topics. | Identified some of the topics. | Picked a topic from the options. |
| 22/08/2018 | Looked up for related papers on digital platforms like Google Scholar and Research Gate. | Read through the papers and saved some for review. | Created a local folder to save the papers as a collection for reference and review. |
| 24/08/2018 | Reading of literature. | Opened collection and read two papers from therein. | Found the predominant topic in them and saved them in a different folder for follow up. |
| 28/08/2018 | Reading of literature. | Read two more papers from the collection. | The topic themes were overlapping and lacked a correlation to my topic of choice, so the two were discarded. |
| 30/08/2018 | Selected the final list of papers to proceed with in the review. | Went through each of the four papers. | Made a list of the final two papers of review. |
| 31/08/2018 | Commencement of assignment. | Began with the citation of relevant sources of the literature review as well as inserting the bibliography. | Identified and inserted only those citations related to the topic under review. |
| 02/09/2018 | Review of the first of the two papers | Carefully read through the paper thrice | Added comments and marked the relevant points and wrote them down in a paper using my own words |
| 03/09/2018 | Review of the second paper | Read through the entire paper thrice and made notes on the key points, theories and ideas | Added comments and marked the relevant points and wrote them down in a paper using my own words |
| 06/09/2018 | Main assignment | Jotted down the highlights from both papers as review | Followed the recommended writing guidelines and formats and prepared the final document |

### 1.1.2 Filing system

*Table 1.2: the filing system from broad scan*

|  |  |  |  |
| --- | --- | --- | --- |
| **Source** | **Keyword** | **Returned literature** | **Collected literature** |
| Google Scholar | Network-based data environments  Mobile data security  Policy transmission | 10100  6030  740 | 3  3  1 |
| Research Gate | Mobile cloud computing  Malware attacks | 350  923 | 1  1 |
| IEEE digital library | Typology of vulnerabilities  Standardized OS | 430  1820 | 1  1 |
| Springer | Data transmission  XML encryption | 1800  3461 | 2  1 |
| Science Direct | Cryptography | 482 | 1 |

### 1.1.3 Bibliographic list from broad scan

Aljudaibi, Samaher. 2016. *Research Paper for Mobile Devices Security*.

10.13140/RG.2.2.32892.13440. Mobile Devices Security; What is Mobile Security, Vulnerabilities, threats and suggested solutions.

Backholm, A., Ahonen, J., Groeber, M., Salorinne, S., Vuornos, L., Saarlilahti, A., Ketonen, M.

and Salmi, P., Seven Networks International Oy, 2010. *Data security in a mobile e-mail service*. U.S. Patent 7,706,781.

Byrne, P. and Kawahara, H., Sun Microsystems Inc, 2007. *Method and system for ensuring*

*mobile data security*. U.S. Patent Application 11/186,578.

Godfrey, J.A., Little, H.A., Brown, M.K., Adams, N.P., Cherry, C.L., Tyhurst, T.R. and Brown,

M.S., BlackBerry Ltd, 2007. *System and method for compressing secure e-mail for exchange with a mobile data communication device*. U.S. Patent 7,254,712.

Heard, R.W., Mann, D.R., Burchett, C.D. and Gordon, I.R., CREDANT TECHNOLOGIES Inc,

2010. *System and method for distribution of security policies for mobile devices*. U.S. Patent 7,665,125.

J. Obiri-Yeboah and M. Qi, "Data security of Android applications," *2016 12th International*

*Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Changsha, 2016, pp. 1716-1721.doi: 10.1109/FSKD.2016.7603436 URL:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7603436&isnumber=7603138>

M. La Polla, F. Martinelli and D. Sgandurra, "A Survey on Security for Mobile Devices,"

in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446-471, First Quarter 2013.doi: 10.1109/SURV.2012.013012.00028 URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6170530&isnumber=6449396>

Shahbazi, M., McAfee LLC, 2013. *Mobile data security system and methods*. U.S. Patent

8,495,700.

Shankar, R., Nadimpalli, B., Swarangi, M., Gudipudi, S., Singh, K. and Deshpande, S.,

Computer Associates Think Inc, 2007. *Method and System for Managing Access to a Wireless Network*. U.S. Patent Application 11/467,803.

Stricklen, M., McHale, T., Caminetsky, M. and Reddy, V., CA Technologies Inc, 2014. *Mobile*

*device management*. U.S. Patent 8,903,365.

Sujithra, M., Padmavathi, G. and Narayanan, S., 2015. Mobile device data security: a

cryptographic approach by outsourcing mobile data to cloud. *Procedia Computer Science*, *47*, pp.480-485.

Taylor, E., Leary, T. and Stockdale, J., IGT Inc, 2012. *Serial advanced technology attachment*

*write protection: mass storage data protection device*. U.S. Patent 8,140,796.

Walker, D., Sapp, K., Goldschlag, D. and Shahbazi, M., Trust Digital LLC, 2011.

*Mobile data security system and methods*. U.S. Patent Application 12/830,861.

Waters, J.D., Mcdonnell, J.T.E., Johnson, I.R. and Baynham, S.H., Hewlett-Packard

Development Co LP, 2008. *Wireless data network security*. U.S. Patent 7,376,384.

Zhang, X., Yang, F., Liu, Z., Wang, Z. and Wang, K., 2010, October. Research and application

of data security for mobile devices. In *International Conference on Computer and Computing Technologies in Agriculture* (pp. 46-56). Springer, Berlin, Heidelberg.

## 1.2 Focused Review

Further research into the topic involved filtering out some of the papers identified and included in the broad scan on the basis of relevance to the topic, “mobile data security”. It is from these eight papers that the researcher selected the final two papers for review.

### 1.2.1 Updated filing system

*Table 1.3: the updated filing system from focused review*

|  |  |  |  |
| --- | --- | --- | --- |
| **Source** | **Keyword** | **returned literature** | **collected literature** |
| Google Scholar | Network-based data environments  Mobile data security | 10100  6030 | 1  2 |
| Research Gate | Mobile cloud computing | 350 | 1 |
| IEEE digital library | Typology of vulnerabilities | 430 | 1 |
| Springer | Data transmission | 1800 | 1 |
| Science Direct | Cryptography | 482 | 1 |

### 1.2.2 Updated bibliography list from focused review

Aljudaibi, Samaher. 2016. *Research Paper for Mobile Devices Security*.

10.13140/RG.2.2.32892.13440. Mobile Devices Security; What is Mobile Security, Vulnerabilities, threats and suggested solutions.

Byrne, P. and Kawahara, H., Sun Microsystems Inc, 2007. *Method and system for ensuring*

*mobile data security*. U.S. Patent Application 11/186,578.

M. La Polla, F. Martinelli and D. Sgandurra, "A Survey on Security for Mobile Devices,"

in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446-471, First Quarter 2013.doi: 10.1109/SURV.2012.013012.00028 URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6170530&isnumber=6449396>

Shahbazi, M., McAfee LLC, 2013. *Mobile data security system and methods*. U.S. Patent

8,495,700.

Sujithra, M., Padmavathi, G. and Narayanan, S., 2015. Mobile device data security: a

cryptographic approach by outsourcing mobile data to cloud. *Procedia Computer Science*, *47*, pp.480-485.

Walker, D., Sapp, K., Goldschlag, D. and Shahbazi, M., Trust Digital LLC, 2011. *Mobile data*

*security system and methods*. U.S. Patent Application 12/830,861.

Waters, J.D., Mcdonnell, J.T.E., Johnson, I.R. and Baynham, S.H., Hewlett-Packard

Development Co LP, 2008. *Wireless data network security*. U.S. Patent 7,376,384.

Zhang, X., Yang, F., Liu, Z., Wang, Z. and Wang, K., 2010, October. Research and application

of data security for mobile devices. In *International Conference on Computer and Computing Technologies in Agriculture* (pp. 46-56). Springer, Berlin, Heidelberg.

## 1.3 Mobile data security and vulnerability

The mobile data sector is an industry currently under rapid expansion and growth. This growth has come with its fair share of challenges and key among them is the security of the data transmitted and stored in mobile devices. Samaher (2016, p. 3-10) was focused on answering the basic questions about what mobile data security is, what it means for mobile data to be vulnerable, various risks in the wake of data vulnerability and how to improve mobile security to deter or prevent or minimize threats to mobile data.

To review the paper, section 1.3.1 is the brief background on the problem, section 1.3.2 reflects upon the approaches employed in the research to get to the proposed solution including methods to mitigate data security risks and finally, section 1.3.3 which is an overview of the entire paper in terms of merits and demerits and a conclusion.

### 1.3.1 Background of the research

In the wake of an expanding mobile industry, security threats have also increased at the same, maybe a faster pace. Despite data security not being a new subject, the level of cyber threats has escalated to a whole new level as a consequence of a rapid increase in mobile device usage and the changes in access and control privileges tagged along with such devices. The author took a contemporary or modern approach to the problem of mobile data security by using a descriptive research methodology. The author is of the opinion that the threats on mobile data security have been on the rise with the increase in sales of mobile devices especially smart phones. Through this, the research introduces the aspect of a positive correlation between increase in mobile devices and mobile data vulnerability.

The paper delves into the aspect of mobile data vulnerability basing the discussion on data exposure levels experienced while using smart phones as compared to other mobile devices (Samaher 2016, p. 5). Exposure to public networks incapacitates antivirus applications and automatic updates as well as diagnostic capabilities of mobile devices, exposing data and personal information to attackers, who use malware to access such information and block any other parties from accessing it. Finally, the research looks into the widespread use of third party applications as the third and a common platform on which attackers hack mobile devices and access personal information.

### 1.3.2 Framework and methodology

The researcher used a descriptive research methodology to paint a picture of what mobile data security and vulnerability looks like. A descriptive analysis takes the form of a discussion on the topic while citing previous research as you found it relevant to the topic. The framework was a discussion of the problem, identification of the challenges in terms of risks and a solution to the challenges identified. The paper approaches the research topic with a systematic description of the various mobile data vulnerabilities, this implying a lack of reasonably significant security. The description of such vulnerabilities is discussed in the form of risks and threats to mobile data security.

The paper identifies a total of eleven situations of mobile data vulnerability. While this research is not going to point out each of the 11 situations, it identifies relevant situations as they relate to the topic. The first situation or threat identified in the paper is data storage. Mobile device users store sensitive and personal information in these devices and still use the same devices to access insecure networks in public places or submit the same information to third party applications on social media platforms.

### 1.3.3 Proposed solution

The author proposes the unification of network architecture in an organization to ensure that both wireless and wired connections all belong to the same network system. A single network system according to the author will enhance a well-secured and highly encrypted network infrastructure. Monitoring of the network is easier when all the connections originate from a single server. In addition, the researcher advocates for a PKI for proper encryption and authentication for instance, setting a minimum threshold for passwords, below which the password cannot be used in the network.

### 1.3.4 Discussion

The researcher is well versed with the various forms of mobile data security and associated vulnerability. The descriptive approach fits the scope of the research and the proposed solutions are relevant to this research. However, the researcher takes a one-sided approach towards data security, without really providing a statistical evidence for the research. The paper is largely descriptive and based on shallow secondary data, making it insufficient for a scientific research on the topic. Finally, the author narrows the scope of the research to smart phones, ignoring the level of vulnerability of data held in other mobile devices.

## 1.4 Cryptographic Approach to Mobile Data Security

This is the second paper that was considered for final review. According to the research, the current level of technology makes the use of mobile devices for our day-to-day lives inevitable. With the increase in usage of mobile devices, comes the increasing need for additional storage of information contained in such devices. The prevalence of cyber threats to data security necessitates a highly-secure and cost-effective way of storing mobile data (Sujithra, Padmavathi & Narayanan 2015, p.483). The paper therefore looks at how secure users can remotely store data in a cloud through cryptographic techniques which reduces the degradation of device performance.

### 1.4.1 Background

The increase in mobile device sophistication consequently calls for sophisticated data storage techniques. The paper introduces the concept of MCC which allows users without enough space on their mobile devices to effectively balance performance and storage capabilities of mobile devices by offloading those files that demand more storage (Sujithra, Padmavathi & Narayanan 2015, p.484). In addition, the increase in customized mobile applications such as banking apps in which sensitive data is contained. The research appreciates the value of mobile data and indentifies the main problem associated with MCC; unauthorized access.

The concern therefore was to enhance cloud data security and at the same time ensure easy access to user data. Mobile gadgets like smart phones have password protection mechanisms on cloud storages to prevent unauthorized access but are limited as they are visible to others. Biometric identifiers are limited to the owner of the data and therefore not helpful in case of an emergency. The research used the constraints to introduce the use of a highly-encrypted algorithm as the most feasible technique to enhance mobile data security.

### 1.4.2 Cryptographic approach

This is a common data protection technique in cloud storage systems. The research identifies the categorization of data into public (sharable) and private (confidential and sensitive) data. The latter is transmitted in an encrypted format through end-to-end encryption. The research therefore proposes the use of different key lengths to encrypt data on the cloud, classifying cryptosystems into symmetric, asymmetric and digital signatures. The symmetric type involves sharing of the encryption and decryption keys which are represented by DES and AES. Asymmetric encryption involves the receiver having a public and private key whereby the former is publishable (Sujithra, Padmavathi & Narayanan 2015, p.480-485). Asymmetric encryption is represented by RSA and ECC.

### 1.4.3 Proposed Hybrid Approach

The paper proposes a solution to the problem of locally encrypting and decrypting data in mobile smart phones’ RAM, a vulnerable storage of data. The proposed approach is a hybrid, 3-tier security encryption using three encryption techniques: MD5 algorithm where the user receives a key (k1), 2nd-tier security is done through AES encryption while the last tier security key is encrypted using ECC algorithm. Combining the different cryptographic algorithms makes up the cloud architecture which according to the researcher gives the user a chance to choose which algorithm to use in encrypting or decrypting data. The effectiveness of the hybrid approach is tested by conducting a statistical analysis using the speed-up ratio:

Speed-up ratio = local processing time – cloud processing time

### 1.4.4 Discussion and conclusion

The cryptographic approach in the research scientifically proves the efficiency of storing mobile data in a cloud rather than locally. In addition, this research tests the hybrid approach in a multiple-system environment, a technique that was never tested before. Mean processing time analysis in the research also proves the efficiency of AES encryption in ensuring mobile data security. Nevertheless, the approach the mean processing and speed-up time parameters used are limited and thus cannot be used to make decisions on the security of the data in cloud platforms.

## 1.5 Final Outline of the Literature Review Chapter

1 introduction

2 Mobile data security and vulnerability

2.1 Background

2.2 Framework and methodology

2.3 Proposed solution

2.4 Discussion

3 Cryptographic approach to mobile data security

3.1 Background

3.2 cryptographic approaches

3.3 Proposed hybrid approach

3.4 Discussion and conclusion

## 1.6 Introduction

The topic of my research is mobile data security. This is a relatively new area in research as mobile devices were not developed long ago. The review of literature involved the carrying out of an extensive search on the internet on the available research papers related to the topic. The research narrowed its focus and scope to come up with two papers for review where the first paper is about mobile data vulnerability in smart phones while the second paper is a cryptographic approach to mobile data security. The second paper is a technical and relatively scientific approach to data security by proposing a hybrid encryption technique for data stored both locally and on the cloud.

# List of references

Aljudaibi, Samaher. 2016. *Research Paper for Mobile Devices Security*.

10.13140/RG.2.2.32892.13440. Mobile Devices Security; what is Mobile Security, Vulnerabilities, threats and suggested solutions.

Sujithra, M., Padmavathi, G. and Narayanan, S., 2015. Mobile device data security: a

Cryptographic approach by outsourcing mobile data to cloud. *Procedia Computer Science*, *47*, pp.480-485.