



**DESIGN OF AN EMAIL AUTO DELETE ALGORITHM THAT
ALLOWS A SENDER TO DELETE SENT MAIL FROM THE
RECEIVERS INBOX FOR ANDROID OPERATING SYSTEM**

BY

KISEMBO MOSES ISAAC

BU/GS16/MCF/6



2016/2019

**A DISSERTATION SUBMITTED TO THE DIRECTORATE OF GRADUATE
TRAINING FOR THE AWARD OF MASTER OF COMPUTER FORENSICS OF
BUSITEMA UNIVERSITY**

DECLARATION

I have composed this report solemnly and has not been submitted in whole or as part in any previous application for the award of a master's degree except where stated or otherwise by reference or acknowledgement.

The work presented is entirely my own.

SIGNED



10/sep/2019

Kisembo Moses Isaac

BU/GS16/MCF/6

Masters of computer forensics candidate

Busitema University



APPROVAL

This research report has been submitted for examination with approval from the following supervisors:


SUPERVISOR

Dr. Ildephonse Nibikora

Busitema University

Faculty of Engineering

Department of computer engineering

SIGN:  DATE: 11/9/2019


SUPERVISOR

Mr. Badru Lusiba

Faculty of Engineering

Department of computer engineering

Busitema University

SIGN:  DATE: 11/09/2019

ACKNOWLEDGEMENT

I would like to thank RUFURUM for the financial support extended towards this research work; your support greatly contributed to the success of this work. To my supervisors, Ildephonse Nibikora, Mr. Badru Lusiba and Ms. Godliver Owomugisha. Thank you! Your academic, moral and professional parenting took me to this last stage. God bless you.

Thank you to my Family, my Parents, my Wife and Daughter, May God bless you for loving me, supporting me and carrying the family responsibility whenever I am academically engaged. Thank you. This work is dedicated to my fallen hero and son Job Kitaka (RIP) who motivated me to work towards this success and my jovial daughter Elizabeth. I love you both dearly. Finally, I wish to thank almighty God for his unconditional love and care. I remain your child forever

TABLE OF CONTENT

DECLARATION	i
APPROVAL.....	ii
ACKNOWLEDGEMENT.....	iii
TABLE OF CONTENT	iv
LIST OF TABLES.....	vii
LIST OF FIGURES.....	viii
LIST OF ACRONYMS.....	x
ABSTRACT.....	xi
CHAPTER ONE: INTRODUCTION.....	1
1.1. Background	1
1.2. Research Problem.....	3
1.3. General Objective/Aim/Purpose	4
1.4. Specific Objectives	4
1.5. Research Questions	4
1.6. Significance of the Research	4
1.7. Research Scope	5
1.8. Justification/Rational	5
1.9. Conceptual Framework.....	6
CHAPTER TWO: LITERATURE REVIEW	7
2.1. Summary of the Chapter.....	7
2.2. Email Communication and Security.....	7
2.3. Client-Server Communication.....	9
2.4. Communication Protocols and Email Protocols	10
2.5. Confidentiality and Privacy	12
2.6. The Existing Confidentiality Technologies.....	13
2.6.1.Pretty Good Privacy (PGP).....	13
2.6.2.End To End Encryption (E2EE).....	15
2.6.3.Whatsapp Delete For All.....	16

2.6.4. Biometric and mobile App Locker Features	17
2.7. Limitations of the Existing Confidentiality Techniques Adoption in Email Communication	18
2.7.1. Weak Cloud Data Protection Laws in the USA.....	18
2.7.2. Mixing Private and Business Communication	18
2.7.3. Lack of Enterprise Administration	18
CHAPTER THREE: METHODOLOGY.....	20
3.1. Introduction	20
3.2. Research Method And Strategy.....	20
3.2.1. Environment: 21	
3.2.2. Design Science Research:.....	21
3.2.3. Knowledge base:.....	22
3.3. The Research Design for this Study	22
3.3.1. Assess Weaknesses of Current Techniques.....	23
3.9 Design Algorithm.....	27
3.9.1 The Greedy Algorithm Approach	28
3.9.2 Evaluation of the Algorithm.....	29
3.10 Ethical Consideration	30
CHAPTER FOUR: GENERAL DISCUSSION	31
4.1. Introduction	31
4.2. The Field Study.....	31
4.3. Reliability Analysis.....	31
4.4. Algorithm Design.....	37
4.4.1 Auto-Delete Message Algorithm	38
4.5. Evaluation of the Developed Algorithm.	40
4.5.1 Description of the Software Application.	42
CHAPTER FIVE: IMPLEMENTATION AND EVALUATION OF THE DEVELOPED ALGORITHM	44
5.1. Introduction	44
5.2. The Software Application Used For the Evaluation	44
5.2.1 Presentation of the Software Application and How It Works	44
5.2.2 Demonstration of How the Mobile Application Runs the Algorithm in Screenshots.....	51

5.3. Assessment of the Algorithm Using Research Questionnaire	51
5.4. SWOT in Information Security	54
5.5. Strength of the Developed Algorithm	57
5.6. Weaknesses of the Developed Algorithm.	58
CHAPTER SIX: DISCUSSION, RECOMMENDATION AND COLUSION	59
6.1. Reflection on the Study.....	59
6.2. Conclusion.....	60
6.3. Recommendations for Future Work.....	60
References	61
APPENDICES	64
Appendix 1: Statistical Outputs	64
Appendix 2: Instruments/Tools	68
Appendix 3: Questionnaire	68

LIST OF TABLES

Table 1: Summary of gaps identified in existing confidentiality techniques.....	17
Table 7: sample population.....	26
Table 8: Sample from the population.....	26
Table 2: Reliability Statistics(Summary of Reliability of Scales (alpha) Measures)	32
Table 3: Questionnaire ONE question coding	64
Table 4: Questionnaire TWO question coding	66
Table 5: identification of client security techniques.....	54
Table 6: analysis of the developed algorithm against existing techniques based on android platform	56

LIST OF FIGURES

Figure 1-1: Conceptual Framework	6
Figure 2-1: Examples of Message Flow	8
Figure 2-2: TCP Protocol Suit Adopted from [13]	10
Figure 3-1: A Diagrammatic Representation of the Theoretical Framework Used In This Research.	21
Figure 3-2: A Class Diagram Describing the Auto Delete Algorithm.....	29
Figure 4-1: Respondent selection from both ICT and non-ICT dependents (n=31).....	33
Figure 4-2: Response on the Existence of Mails That Deserve To Be Deleted (A4) (Source: Primary Data).....	34
Figure 4-3: Existence of mails that the auto wipe algorithm should have deleted (A5). Source: Primary Data	35
Figure 4-4: Existence of Sensitive Email Content on User Inbox that are Only Safer When Deleted (A6). Source: Primary Data	35
Figure 4-5: People who delete mails as a form of ensuring confidentiality (A7). Source: Primary Data.....	36
Figure 4-6: People who ask their email receivers to delete (A8). Source: Primary Data	36
Figure 4-7: Technical response on the state of security on the email clients B4, B5, B9. Source: Primary Data.....	37
Figure 5-1: A flow chart giving a description of the algorithm.....	41
Figure 5-2: A flow chart giving a description of how the software application works	43
Figure 5-3: A use case describing the functionality of the algorithm.....	43
Figure 6-1: The systems icon in the screen.....	45
Figure 6-0: The main menu.....	45

Figure 6-2: The attachment upload.....	46
Figure 6-3: Recipient Selection	47
Figure 6-4: Expiry time setting.....	48
Figure 6-5: Refreshing contacts.....	49
Figure 6-6: The message typing.....	49
Figure 6-7: Message sending	50
Figure 6-8: Evaluation on the application.....	51
Figure 4-8: Data Wipe Algorithm Evaluation Chart.....	52
Figure 4-9: Percentage of Responses on the algorithm evaluation.....	53

LIST OF ACRONYMS

SSL	Secure Socket Layer
PGP	Pretty Good Privacy
E2EE	End to End Encryption
TLS	Transport Layer Security
SMTP	Simple Mail Transfer Protocol
FTP	File Transfer Protocol
SSH	Secure Shell
HTTP	Hyper Text Transfer Protocol
ARPNET	The Advanced Research Projects Agency Network
UBOS	Uganda Bureau of Statistics
NITA-Uganda	National Information Technology Authority-Uganda
OS	Operating System
RFC	Request for Comments
MUA	Mail User Agent
MTA	Mail Transfer Agent
DNS	Domain Name System
LDA	Local Delivery Agent
IP	Internet Protocol
DoD	Department of Defense
ARPA	Advanced Research Projects Agency
UDP	User Datagram Protocol

ABSTRACT

Although email is a valuable tool, it creates security challenges when not properly managed. There is a growing adoption of email as official form of communication in many organizations with majority of users on mobile android devices. Banks, health care and many other service providers are communicating to their clients through email in which they share sensitive and confidential information. One major threat is that email users lack confidentiality on their emails accessed via android mobile due to weaknesses of android OS platform that is easy to penetrate by hackers and android email client that presents a onetime login and password authentication can only be required again if the email account is deleted from the android mobile device. In this study, we designed an algorithm and implemented on an android application that allows an email sender to compose an email and set the time the email will stay in the receiver inbox before it automatically wipes off. The researcher prepared a questionnaire that was shared with the email users, the users comprised of those with email technical background and those that are typical email users and we were able to get their opinion on the lack of confidentiality on the android mobile email. We also engaged them in testing and evaluating of the algorithm where they were able to confirm that the algorithm addresses the confidentiality threat on the android email clients. The algorithm has been found to address the confidentiality challenge that android mobile platforms face and users recommended it to be incorporated into email standard operation process to avoid old yet confidential information from remaining in user inbox

CHAPTER ONE: INTRODUCTION

1.1. Background

Communication is the imparting or exchanging of information by speaking, writing, or using some other medium [1]. Communications is a means of sending or receiving information, such as telephone lines or computers [2]. [1]. Communication is said to have occurred when one individual action provide a signal that changes the behavior if another individual [2]. Since the 1960s when the globally interconnected computers were established, ARPNET then became the largest operational network on which several [3]. Internet and the many smaller networks that connect to it have availed the several communication technologies to the people such as electronic mail and bulletin boards, teleconferencing, information utilities, and the many others that they offer [3]. Unlike the telephone, radio, and television, computer networks are used for both point-to-point and broadcast communications [3]. Electronic mail tends to be used for person-to-person communication; that is to say, messages are sent to specified individual recipients although they can also be readily sent to groups of recipients. Electronic bulletin boards are used to post messages that can be read by anyone who has access to the boards on which they are posted [3].

Internet has penetrated up to 54.4% of the world with Africa at 35.2% and UBOS putting the rate of internet penetration in Uganda at 34.6% [4] , the statistics indicate growth in the use of internet based services [5]. Email is a means of communication and is an internet service with a rise in its adoption, Forbes published that the email penetration is hitting 62% and that majority of users are accessing via smart phones due to their reliability and young people are using emails more that the elders. According to NITA-Uganda, 96.1% of ministries, departments and agencies give email addresses to their employees with 94.6% using email for official communication and 62.9% enforcing email use. This statistic also shows that there is need to address security issues around emails as the email usage is becoming high. With the increased adoption rate of the email use, there is a growing concern of privacy and confidentiality of email especially, considering the way smartphones provide access to emails demonstrates high dependency on the security of the platform (OS) which is easy to compromised due to the human social nature of sharing phones and other known platform (OS) weaknesses. It is known that, majority of users accessing their email

References

- [1] Oxford University, The English Oxford Dictionaries (OED), London: Oxford University Press.
- [2] T. HALIDAY and P. SLATTER, "INFORMATION AND MANIPULATION," in *EVOLUTION OF COMMUNICATION*, LONDON, BLACKWELL SCIENTIFIC PUBLICATION, 1983, p. 157.
- [3] R. S. Nickerson, "Communication Technology and Telenetworking," in *Emerging Needs and Opportunities for Human Factors Research*, Washington DC, NATIONAL ACADEMY PRESS, 1995, p. 177.
- [4] UBOS, "Communication," 18 March 2018. [Online]. Available: <https://www.ubos.org/explore-statistics/statistical-datasets/4533/>.
- [5] "Internet World Stat-Usage and Population Statistics," 31 December 2017. [Online]. Available: <https://www.internetworldstats.com/stats1.htm>.
- [6] 31 March 2019. [Online]. Available: <http://gs.statcounter.com/os-market-share/mobile/worldwide>.
- [7] M. Tracy, W. Jansen, K. Scarfone and J. Butterfield, "Guidelines on Electronic Mail Security," National Institute of Standards and Technology, MD 20899-8930, Gaithersburg, 2007.
- [8] T. KRISTIJAN, "Secure Email Client," THE UNIVERSITY OF SHEFFIELD CITY LIBERAL STUDIES, 2006.
- [9] "Hacker exposes ex-US President George H W Bush emails," BBC News, February 2013. [Online]. Available: <https://www.bbc.com/news/world-us-canada-21380393>. [Accessed 12 March 2019].
- [10] A. News, "News of the World Is No More," ABC News, 2011. [Online]. Available: <https://abcnews.go.com/International/news-world-closed-telephone-hacking-scandal/story?id=14037284>. [Accessed 12 March 2019].
- [11] A. Hevner, "Design Science in Information Systems Research," *Research Gates*, pp. 79-80, 2014.
- [12] Ivana, "SECURE SISS DATA," 14 December 2017. [Online]. Available: <https://securerwissdata.com/secure-email-works/>.
- [13] P. B. Nath and M. Uddin, "TCP-IP Model in Data Communication and Networking," *American Journal of Engineering Research (AJER)*, 2015.
- [14] GradesFixer., "Confidentiality, Integrity, and Availability (CIA triad).," 19 November 2018.
- [15] F. McGrath, "98% of Digital Consumers are Social Networking," 16 March 2019. [Online]. Available: <https://blog.globalwebindex.com/chart-of-the-day/98-of-digital-consumers-are-social-networking/>.
- [16] D. Chaffey, "Global social media research summary 2019," 16 March 2019. [Online]. Available: <https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>.

- [17] P. Zimmermann, "Pretty Good Privacy," 16 March 2019. [Online]. Available: https://en.wikipedia.org/wiki/Pretty_Good_Privacy.
- [18] M. Rouse, "Pretty Good Privacy (PGP)," 16 March 2019. [Online]. Available: <https://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy>.
- [19] Q. NORTON, "Email Is Dangerous," 16 March 2019. [Online]. Available: <https://www.theatlantic.com/technology/archive/2018/05/email-is-dangerous/560780/>.
- [20] "HACKER LEXICON: WHAT IS END-TO-END ENCRYPTION?," 16 March 2019. [Online]. Available: <https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>.
- [21] "End-to-end encryption," 16 March 2019. [Online]. Available: https://en.wikipedia.org/wiki/End-to-end_encryption.
- [22] J. Lindsay, "Does WhatsApp delete for everyone have a time limit? What can the other people see?," 14 July 2018. [Online]. Available: <https://metro.co.uk/2018/07/14/whatsapp-delete-everyone-time-limit-can-people-see-7716098/>.
- [23] Jonathan A. Obar and Steven Wildman, "Social Media Definition and the Governance Challenge: An Introduction to the Special Issue," January 2015.
- [24] AVI_CICIREANU, "The Disadvantages of Using WhatsApp for Business," 16 March 2019. [Online]. Available: <https://brandminds.ro/the-disadvantages-of-using-whatsapp-for-business/>.
- [25] Andreas M. Kaplan and Michael Haenlein, "Users of the world, unite! The challenges and," 2010.
- [26] "Government e-Service Delivery: Identification of Success Factors from Citizens' Perspective," Luleå University of Technology, 2008.
- [27] M. EDWARD, "A Model of e-Health Acceptance and Usage in Uganda: The perspective of Online Social Networks," Makerere University, Kampala, 2015.
- [28] Joint Research Centre (JRC), "My Email Communications Security Assessment (MECSA): 2018 Results," European Union, Luxembourg, 2019.
- [29] C. E. SHANNON, "A Mathematical Theory of Communication," [Online]. Available: <http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf>.
- [30] V. Beal, "OSI - Open System Interconnection," 11 March 2019. [Online]. Available: <https://www.webopedia.com/TERM/O/OSI.html>.
- [31] "Communication," 11 March 2019. [Online]. Available: <https://en.wikipedia.org/wiki/Communication>.
- [32] J. M. ADELMAN, "A Constitutional Conveyance of Intelligence, Public and Private": The Post Office, the Business of Printing, and the American Revolution".
- [33] Jan Kietzmann, Kristopher Hermkens, Bruno Silvestre and Ian Paul McCarthy, "Kietzmann, Jan H.; Kristopher Hermkens (2011). "Social media? Get serious! Understanding the functional building blocks of social media". Business Horizons. 54 (3): 241-251. doi:10.1016/j.bushor.2011.01.005."

- [34] "Sarah Palin email hack," Wikipedia, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Sarah_Palin_email_hack. [Accessed 12 March 2019].
- [35] "In Kampala, man arrested over hacking into emails, stealing over Shs80m," 13 March 2019. [Online]. Available: <https://www.sautitech.com/digital/in-kampala-man-arrested-over-hacking-into-emails-stealing-over-shs80m/>.
- [36] "Social Network Sites: Definition, History, and Scholarship," 1 October 2007. [Online]. Available: <https://academic.oup.com/jcmc/article/13/1/210/4583062>.
- [37] Eugene Agichtein, Carlos Castillo, Debora Donato, Aristides Gionis and Gilad Mishne, "Finding High-Quality Content in Social Media," *WSDM*, 2008.
- [38] J. V. Pavlik and S. McIntosh, *Converging media : a new introduction to mass communication*, New York: Oxford University Press, 2019.
- [39] D. P. Agrawal and Q. Zeng, *Introduction to wireless and mobile systems*, Toronto: Ontario: Thomson, 2006.
- [40] J. F. ... K. ... and K. W. Ross, *Computer Networking: A Top-down Approach Featuring the Internet*, Amsterdam: Addison-Wesley Longman, 2003.
- [41] "An Introduction to Cryptography," United States .
- [42] C. E. SHANNON, "Communication Theory of Secrecy Systems," [Online]. Available: <http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>.
- [43] M. H. S. and A. R. Reddy, "Performance Analysis of AES and MARS Encryption," *International Journal of Computer Science Issues*, 2011.
- [44] A. L. (NIST), "Guideline for Implementing Cryptography in the Federal Government," *COMPUTER SECURITY RESOURCE CENTER*, 1999.
- [45] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti and E. Roback, "Report on the Development of the Advanced Encryption Standard (AES)," *Journal of Research of NIST*, 2001.
- [46] M. F. Wali and M. Rehan, "Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)," in *2005 Student Conference on Engineering Sciences and Technology*, Karachi, Pakistan, 2005.
- [47] J. F. H. Jr., W. C. Black, B. J. Babin and R. E. Anderson, *Multivariate Data Analysis*, EDINBURG: Edinburgh Gate, 2014.
- [48] O. M. A. Al-Hazaimeh, "Increase the Security Level for Real-Time Application Using New Key Management Solution," *IJCSI International Journal of Computer Science Issues*, 2012.
- [49] R. Hunt, "PKI and digital certification infrastructure," in *Proceedings. Ninth IEEE International Conference on Networks, ICON 2001*, Bangkok, Thailand, 2002.
- [50] WhatsApp, "WhatsApp Encryption Overview," 19 Mar 2019. [Online]. Available: <https://www.whatsapp.com/security/>.
- [51] Kaspersky, "Kaspersky Lab Statistics," 1 May 2019. [Online]. Available: <https://securelist.com/statistics/>.