

**Secure Mobile Collaboration Platform
for Transmission and Archival of
Medical Images**

by

Tholka Mudalige Kasun Kosala Jinasena

Ph.D.

2018

**Secure Mobile Collaboration Platform
for Transmission and Archival of
Medical Images**

by

Tholka Mudalige Kasun Kosala Jinasena



Ph.D.

2018

Declaration

The work described in this thesis was carried out by me under the supervision of Prof. R.G.N. Meegama, Department of Computer Science, Faculty of Applied Sciences, University of Sri Jayewardenepura and Dr. R.B. Marasinghe, Department of Medical Education & Health Sciences, Faculty of Medicine, University of Sri Jayewardenepura and a report on this has not been submitted in whole or in part to any university or any other institution for another Degree/Diploma.



.....
Signature of Candidate

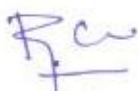
T.M.K.K. Jinasena

Date: ...21../...02../...2019

Certification of the Supervisors

We certify that the candidate has incorporated all corrections, additions and amendments recommended by the examiners to this version of the Ph.D. thesis.

Supervisor : Prof. Ravindra Gayan N. Meegama.



Date: 21/02/2019

Signature of Supervisor

Prof. R. G. N. MEEGAMA
Department of Computer Science
Faculty of Applied Sciences
University of Sri Jayawardenepura
Nugegoda - Sri Lanka.

Co-Supervisor : Dr. Rohana Basil Marasinghe.



Date: 21/02/2019

Signature of Co-Supervisor :

DR. R. B. MARASINGHE
HEAD
DEPT. OF MEDICAL EDUCATION
Faculty of Medical Sciences
University of Sri Jayawardenepura
Gangodawila, Nugegoda,
Sri Lanka.

Table of Content

Table of Content	i
List of Figures	vi
List of Tables	ix
List of Equations	xi
List of Acronyms	xii
Acknowledgement	xiv
ABSTRACT.....	xv
Chapter 1 INTRODUCTION.....	1
1.1 Introduction	1
1.2 Motivation	4
1.3 Research Problem.....	5
1.4 Aims and Objectives	7
1.5 Scope and Limitations	8
1.6 Organization of the Report.....	8
Chapter 2 Literature review	9
2.1 Mathematics behind the Security	9
2.1.1 Number Theory in Cryptography.....	9
2.1.2 Random Number Generation	16
2.1.3 Abstract Algebra in Cryptography.....	19
2.1.4 Group Theory.....	21
2.1.5 Ring Theory	22
2.1.6 Field Theory.....	23
2.1.7 Galois Field.....	23
2.1.8 Time Complexity	26

2.1.9	Discrete Logarithms.....	28
2.1.10	Discrete Logarithm Problem (DLP).....	31
2.1.11	Pollard Rho Algorithm for Logarithms.....	33
2.2	Computer Security.....	34
2.3	Cryptography.....	37
2.3.2	Confusion and Diffusion.....	41
2.3.3	AES Encryption	46
2.3.4	Attacks on RSA.....	55
2.3.5	Elliptic Curve Cryptography.....	57
2.3.6	Access Control.....	81
2.3.7	Digital Rights Management	85
2.3.8	Digital Certificates and Public key Infrastructure	86
2.3.9	Attribute-Based Encryption (ABE).....	90
2.3.10	Multicasting	91
2.4	Libraries and APIs.....	92
2.4.1	OpenSSL.....	92
2.4.2	Bouncy Castle and Spongy Castle Libraries.....	92
2.4.3	WebRTC	93
2.5	Health Informatics.....	96
2.5.1	eHealth Privacy and Security.....	96
2.5.2	HL7	97
2.5.3	HL7 Messages.....	97
2.5.4	Personal Health Information Protection Act, 2004 (PHIPA).....	100
2.5.5	Health Insurance Portability and Accountability Act (HIPAA)	100
2.5.6	Digital Imaging and Communications in Medicine.....	101

2.5.7	Picture Archival Communication System (PACS)	105
2.6	Similar Systems.....	108
2.6.1	Osirix.....	108
2.6.2	Mobile MIM.....	109
2.6.3	Mango	110
2.6.4	Sony PlayStation.....	111
2.6.5	Windows Media Digital Rights Management (WM-DRM)	111
2.6.6	Open PGP and GPG.....	112
Chapter 3 Methodology		113
3.1	ADDIE	113
3.2	Analysis Phase.....	113
3.3	Design Phase	115
3.3.1	Design of Questionnaires and Hypotheses	115
3.3.2	Design of the System Architecture	117
3.3.3	Design of the Public key Infrastructure	119
3.3.4	Design of the Picture Archival Communication System.....	120
3.3.5	Design of the Proposed Secure Mechanism.....	121
3.3.6	Design of Integrity Checking and Authentication	127
3.3.7	Design of the Proposed File Structure	127
3.4	Algorithms.....	129
3.4.1	Kasun's Algorithm of Multi-key Encryption for Multicasting.....	131
3.4.2	Design of the Mobile Application.....	136
3.4.3	Implementation Phase.....	139
3.4.4	Implementation of Questionnaires and Hypotheses	139
3.4.5	Implementation of the System Architecture	140

3.4.6	Public key Infrastructure	141
3.4.7	Picture Archival Communication System.....	143
3.4.8	Proposed Secure Mechanism	144
3.4.9	Proposed File Structure	144
3.4.10	Mobile Application	145
3.4.11	Image Manipulation and the DICOM Library	145
3.4.12	Socket Programming and WebRTC.....	145
3.4.13	Evaluation	146
Chapter 4 Results and Discussion.....		147
4.1	Requirements of Stakeholders.....	147
4.1.1	Requirement of the Mobile Collaborative Environment	147
4.1.2	Public Key Infrastructure	154
4.1.3	Picture Archival Communication System.....	159
4.1.4	The Cryptography and the Proposed Secure Mechanism	160
4.1.5	The Performance Analysis of the Cryptography in Communication.....	182
4.1.6	The Most Significant Invention of the Research	187
4.1.7	The Proposed File Structure.....	188
4.1.8	The Mobile Application	189
Chapter 5 Conclusions		195
5.1	Major Achievements	195
5.1.1	A New Algorithm for Multi-key Encryption for Multicasting	196
5.1.2	DICOM Library for Android and Java Users	196
5.1.3	Customized Image View with Gesture Event Handler	196
5.1.4	Peer to Peer Communication Library	197
5.1.5	Real-time Interactive Whiteboard.....	197

5.1.6	PKI Tool for Digital Certificate Generation	198
5.2	Recommendations	199
5.2.1	Enhanced DICOM Library	199
5.2.2	PKI Tool for Mobile and Plug-in for Common Applications.....	199
5.2.3	HL7 Enabled File Structures.....	199
	REFERENCES	200
	Appendix 1.....	247
	Appendix 2.....	252

List of Figures

Figure 2.1.7.1: Elements of the Finite Field \mathbb{Z}_{13}	25
Figure 2.1.8.1: Time Complexity vs Key Size.....	27
Figure 2.1.11.1: Categories of Threats.....	34
Figure 2.1.11.2: Overview of the Information Security.....	35
Figure 2.1.11.3: Attacks on CIA.....	36
Figure 2.1.11.1: Evolution of Cryptography and Cryptanalysis	37
Figure 2.3.2.1: S-box	42
Figure 2.3.2.2: P-boxes: Straight, Expansion, and Compression.....	43
Figure 2.3.2.3: Other Components of Modern Block Ciphers.....	44
Figure 2.3.2.4: Basic Structure of a Product Cipher	44
Figure 2.3.3.1: AES Algorithm.....	48
Figure 2.3.3.2: Structure of each Round of AES	51
Figure 2.3.3.3: Detail View of an AES Round	52
Figure 2.3.3.4: Comparison of Encryption and Decryption Processes of AES	55
Figure 2.3.5.1: Different Elliptic Curves Over \mathbb{R}	59
Figure 2.3.5.2: An Elliptic Curve over a Finite Field \mathbb{Z}_p , p -Prime	60
Figure 2.3.5.3: Different Elliptic Curves	62
Figure 2.3.5.4: Addition of Two Distinct Points on the Elliptic Curve.....	64
Figure 2.3.5.5: Addition a Point to Itself	66
Figure 2.3.5.6: Doubling Point P Repeatedly to find 4P	66
Figure 2.3.5.7: Valid Points of $E(\mathbb{Z}_{13})$	68
Figure 2.3.5.8: Point at Infinity.....	69
Figure 2.3.5.9: $y^2 = x^3 + 2x + 2 \pmod{17}$ over \mathbb{Z}_{17}	72
Figure 2.3.8.1: CA and Digital Certificates	87

Figure 2.3.8.2: Certificate Authority Hierarchy.....	88
Figure 2.4.3.1: STUN Server	94
Figure 2.4.3.2: TURN Server.....	94
Figure 2.4.3.3: STUN, TURN, and ICE	95
Figure 2.4.3.4: TURN based Media Replay in WebRTC	95
Figure 2.5.6.1: XML vs DICOM	101
Figure 2.5.6.2: Information Model of DICOM.....	102
Figure 2.5.6.3: Structure of a DICOM File.....	103
Figure 2.5.6.4: Information Entities of DICOM	103
Figure 2.5.7.1: Standards and Frameworks for Interoperability	106
Figure 2.5.7.2: Interconnectivity of Servers	107
Figure 3.3.2.1: Proposed System Topology	118
Figure 3.3.3.1: CA and Digital Certificates	120
Figure 3.3.7.1: Proposed File Structure	128
Figure 3.4.2.1: Overview of the Image Visualization App.....	137
Figure 4.1.2.1: Key Generation.....	156
Figure 4.1.2.2: Signing Certificates	158
Figure 4.1.4.1: (Left) Input Parameters and (Right) Performance Results of AES Benchmark Tests	161
Figure 4.1.4.2: Mean AES Encryption Time vs Key Size	165
Figure 4.1.4.3: Mean AES Decryption Time vs Key Size.....	165
Figure 4.1.4.4: 128 bits RSA Key Generation Time vs Frequency	167
Figure 4.1.4.5: 256 bits RSA Key Generation Time vs Frequency	167
Figure 4.1.4.6: RSA Key Generation Time vs Key Size	167
Figure 4.1.4.7: Boxplot of RSA 4096 bits Key Generation Times.....	168

Figure 4.1.4.8: Median RSA Key Generation Time vs Key Size	169
Figure 4.1.4.9: Benchmark to Test ECC and RSA Performances	170
Figure 4.1.4.10: List of Supported Curves.....	171
Figure 4.1.4.11: (Left) EC Key Generation, (Right) EC Diffie-Hellman Key Exchange	172
Figure 4.1.4.12: Elliptic Curve vs Key Generation Time	173
Figure 4.1.4.13: EC Key Size and ECDH Time	175
Figure 4.1.4.14: Brainpool Curves Field Size vs ECDH Time.....	176
Figure 4.1.4.15: RSA Key Size vs Mean Sign Time	178
Figure 4.1.4.16: RSA Key Size vs Mean Verify Time	178
Figure 4.1.5.1: Image Sizes (bytes)	184
Figure 4.1.5.2: Encryption & Decryption Times	185
Figure 4.1.5.2: Round-Trip Times (ms).....	185
Figure 4.1.5.2: One-Way Communication Times vs Images.....	186
Figure 4.1.8.1: Login Screen of the Mobile App.....	189
Figure 4.1.8.2: (Left) File Browser (Right) Interactive Whiteboard	190
Figure 4.1.8.3: (Left) Change the Brush Size (Right) Change the Drawing Color	191
Figure 4.1.8.4: Video Conferencing with Peers: (Left) All Users (Right) Full Screen View	192
Figure 4.1.8.5: Mean Satisfaction Frequency	194

List of Tables

Table 2.3.3.1: AES S-box	50
Table 2.3.3.2: Brute Force Attack on AES (Key Size vs Time)	54
Table 2.3.4.1 : Potential Attacks on RSA	56
Table 2.3.5.1: Comparable Key Sizes for Equivalent Security	59
Table 2.5.3.1: Delimiter Characters used in HL7	99
Table 4.1.1.1: Usefulness of Teleradiological Systems	148
Table 4.1.1.2: Benefits of Teleradiological Systems	149
Table 4.1.1.3: Problems of Implementing Teleradiological Systems in Sri Lanka	150
Table 4.1.1.4: Frequency of using ICT	152
Table 4.1.1.5: Lack of ICT Facilities for the Implementation of Teleradiological Systems is Sri Lanka	153
Table 4.1.2.1: PKI Questionnaire Responses of Usability of Command Line	155
Table 4.1.2.2: Feedbacks of Usability of GUI Tool vs Command Line	157
Table 4.1.4.1: Minimum AES Times	162
Table 4.1.4.2: AES Encryption/Decryption Length vs File Size (bytes)	162
Table 4.1.4.3: AES Encryption and Decryption Times (ms) vs Key Size (bits)	164
Table 4.1.4.4: RSA Key Size vs Key Generation Time	166
Table 4.1.4.5: ECC Curve Vs Key Generation Time	173
Table 4.1.4.6: Curve Vs ECDH Run Time	174
Table 4.1.4.7: RSA Sign and Verification Times (ms) and Sign Size (Byte) Vs Hash Algorithm	177
Table 4.1.4.8: ECC Sign and Verification Times (ms) and Sign Size (Byte) Vs Hash Algorithm	179
Table 4.1.5.1: Communication Times vs Image Size (bits)	183

Table 4.1.5.2: Communication Times, AES Encryption Times (ms) vs Image Size	183
Table 4.1.5.3: Communication Times, AES Encryption and Decryption Times (ms) vs Image Size (bytes).....	184
Table 4.1.8.1: Responses of Mobile App Effectiveness	193

List of Equations

Equation 3.3.5.1: Calculate Access Key using the Master Key.....	125
Equation 3.4.1.1: Calculate Polynomial using Lagrange Interpolation	131
Equation 3.4.1.2: General form of the Resultant Polynomial.....	131
Equation 3.4.1.3: Secret Session key Generation	132

List of Acronyms

ABE	Attribute-Based Encryption
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
AES	Advanced Encryption Standard
CA	Certification Authority
CIA	Confidentiality, Integrity, and Availability
CRHF	Collision Resistant Hash Functions
CSPRNG	Cryptographically Secure Pseudo-Random Number Generators
CT	Computed Thermography
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
DLP	Discrete Logarithm Problem
DRM	Digital Rights Management
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EMR	Electronic Medical Records
GF	Galois Field
GPG	GNU Privacy Guard
GPL	General Public License
HIS	Health Information Systems
HL7	Health Level Seven

HMAC	Keyed-Hash Message Authentication Code
IFP	Integer Factorization Problem
L2TP	Layer Two Transport Protocol
MAC	Message Authentication Codes; Mandatory Access Control
MD	Message digests
MIDT	Medical Identity Theft
MRI	Magnetic Resonance Imaging
NIST	National Institute of Standards and Technology
OWHF	One-Way Hash Functions
PACS	Picture Archival Communication System
PET	Positron Emission Tomography
PGP	Pretty Good Privacy
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generators
ROI	Region of Interest
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithms
SPN	Substitution-Permutation Network
SSL/TLS	Secure Sockets Layer/Transport Layer Security
US	Ultrasound
VPN	Virtual Private Network
WebRTC	Web Real-Time Communication
WM-DRM	Windows Media Digital Rights Management

Acknowledgement

First, I wish to dedicate my deeper appreciation to my supervisors Prof. R.G.N. Meegama and Dr. R.B. Marasinghe for their excellent support and guidance towards the success of my goals. Also I owe my gratitude to Dr. Wickrananayake for his continues support towards the success of this research. They spend their valuable time to listen to my ideas, gave me their valuables comments and direct me to the correct path. They always encourage and lift me whenever I fell down.

I would also like to convey my gratitude towards Mr. Dias, and Mrs Hasanthi for giving me their full hand for questionnaires preparation, result analysis and all the statistical works. Moreover, Ms Kasuni, Mr Gunarathne, and Dr. Sanjeewa for their tremendous supports for mathematical works and proof readings of this research. Further, I highly appreciate the generous supports of Dr. Fernando, Mr Harsha, Mr Charitha, and Mr Gayan for servers and infrastructure matters. Finally, I owe my gratitude to all the academics, colleagues, and friends who supported me in various ways to make this research a success. Without their kind support, and encouragements, this research would never have been successfully completed.

I also offer my gratefulness to all the community and individuals who supported me and devoted their valuable time towards this research. Finally, I am grateful to open source community, research community, and all the authors of references for making available their findings to the others for the betterment of the mankind.

Secure Mobile Collaboration Platform for Transmission and Archival of Medical Images

T.M.K.K. Jinasena

ABSTRACT

With the advancement of technology, the digital health systems are becoming popular among the service providers as well as the consumers alike. Ubiquitous access of internet and mobile devices allow people to access necessary data irrespective of their physical location and the time. This ensures location transparency for their personal and professional duties. On the contrary, this creates vulnerabilities in confidentiality, integrity, and availability especially when sensitive data such as medical and health related data are being transfer over public networks such as internet and mobile networks. It is evident that, the privacy and security issues have become a significant barrier when developing digital health systems. Especially, securing large medical data such as medical images in relatively less powerful devices such as mobile devices is challenging. Mere securing data is insufficient for interactive real-time collaborative discussions sessions in medicine. It needs efficient, robust cryptosystem to assure security services such as digital authentication, dynamic access control, integrity verification, non-repudiation, etc. Moreover, the latest reviews highlight that the present secure mechanisms have been threaten by the rapid advancement of technology and improved algorithms. Therefore, the primary focus of this research is to invent a novel, robust secure mechanism to provide above features.

The requirements and the present status of the research problem have been identified through the literature review, structured interviews, and the questionnaires. The elliptic curve

cryptography has been chosen as the cryptographic method for the research. Next, a public key infrastructure was established by setting up a hierarchy of certificate authorities and issuing digital certificates to all the users and the servers. A GUI tool was developed to support digital certificate management. A picture archival and communication system server was established and populated with sample images. Then, an Android-based mobile application was developed to view those medical images remotely through the VPN connections. The app was empowered with collaborative features and an interactive whiteboard in order to conduct real-time interactive discussion with remote experts. This research introduces five access control methods together with a file structure to enforce the access control for multiple users through the same content. An app was developed to test the selected algorithms and the proposed cryptographic work in a mobile environment. Moreover, the usability of the developed tool and the app were tested. The results were critically analyzed.

Results show that the lack of developments in elliptic curve cryptography algorithms in Android. Practical results do not show any significant efficiency in cryptographic work due to un-optimized libraries. In conclusion, this study provide evidence on a successful, novel, robust algorithm based on elliptic curve cryptography to enforce the access control for multiple users through the same content. Additionally, a public key infrastructure management tool, a medical image conversion library and an interactive whiteboard for Android users have been developed for the benefit of future researchers and the open source community.

Keywords: Elliptic Curve Cryptography, Access Control, Digital Rights Management, Mobile Computing, Tele-Radiology