

UNIVERSITI TENAGA NASIONAL LIBRARY

**DESIGN AND IMPLEMENTATION OF SECURE SOLUTION FOR M-
GOVERNMENT ON MOBILE PLATFORMS USING HYBRID OF NTRU-
PKI AND AES-RIJNDAEL**

By

MALIK ANAS TAWFEEQ

**A Dissertation Submitted in Fulfillment of
the Requirement for the Degree of Master of Information Technology
College of Graduate Studies
Universiti Tenaga Nasional**

December 2013

- ① Internet in public administration
- ② Electronic government information

THS
JF
1525
.A8
M3V
2013

UNIVERSITI TENAGA NASIONAL LIBRARY

UNITEN LIBRARY

Property of UNITEN Library.
Action will be taken against any user who
underlines words, makes notes in the
margins or disfigures or damages books in
any way.

DATE RECEIVED : 01 JUN 2014

ACCESSION NO : 160655

ABSTRACT

In recent years and specifically in the era of rapid technology development, many changes have taken place in the field of communication technologies (ICT), where mobile devices have replaced computers in multiple significant tasks. This has influenced the interactions between citizens and government agencies in what is called the m-Government, which is an extension of the e-Government that provides services to citizens in general or subscribers in particular. As these services range from public to private bodies and data transmitted sometimes require authentication and confidentiality, the need to secure them has been found to be inevitable. In this dissertation, the author proposes a technique to secure the transmission of the Electronic Medical Records using hybrid security algorithms of AES-Rijndael and NTRU, since with concentration on confidentiality and authentication as core services in m-Government current transactions, in order to enhance the security of transmission medium and achieve better security of m-Government services. The findings of this dissertation have shown proof of the powerful presence of security factors concerning confidentiality and authentication in the field of m-Government, and test performance approves that the proposed technique is applicable on smartphone devices.

DECLARATION

I hereby declare that this thesis, submitted to Universiti Tenaga Nasional as fulfillment of requirements for the degree of Master of Information Technology has not been submitted as an exercise for a similar degree at any other university. I also certify that the work described here is entirely my own except for excerpts and summaries whose sources are appropriately cited in the references.

This thesis may be made available within the university library and may be photocopied or loaned to other libraries for the purposes of consultation.

December 2013

MALIK ANAS TAWFEEQ

TABLE OF CONTENTS

ABSTRACT	ii
ACKNOWLEDGMENT	iii
DECLARATION.....	iv
LIST OF ABBREVIATIONS.....	x
CHAPTER 1 INTRODUCTION	
1.1 Introduction.....	1
1.2 Research background	2
1.3 Research Problem Statement	4
1.4 Research Objectives	6
1.5 Research Questions	7
1.6 Research Scope	7
1.7 Organization of Thesis	8
CHAPTER 2 LITERATURE REVIEW	
2.1 Introduction.....	10
2.2 Mobile Government (m-Government)	11
2.3 Information Security	14
2.4 Electronic Medical Records (EMR).....	18
2.5 Confidentiality	21
2.6 Authentication.....	24
2.7 Cryptography	27
2.8 Symmetric Cryptography Algorithms	29
2.8.1 Data Encryption Standard (DES)	31
2.8.2 Triple DES.....	33
2.8.3 Advanced Encryption Standard (AES) / Rijndael	33
2.8.4 Comparison of Symmetric Encryption AES, 3DES AND DES.....	35
2.9 Asymmetric Cryptography Algorithms.....	38
2.9.1 RSA (Ravest, Shamir, Adleman).....	39
2.9.2 NTRU Algorithm (Nth Degree Truncated Polynomial Ring Units)	40

2.9.3 Elliptic Curve Cryptography (ECC)	42
2.9.4 Comparison of RSA, ECC and NTRU	42
2.10 Digital Envelope Method.....	46
2.11 Chapter summary	48
CHAPTER 3 RESEARCH METHODOLOGY	
3.1 Introduction.....	50
3.2 Research Phases	50
3.3 Literature Review	53
3.4 Hybrid Technique Justification -The Proposed Model	53
3.5 Case Study	59
3.6 Data collection tools.....	59
3.6.1 Hardware tools.....	60
3.6.1.1 Desktop Computer:	60
3.6.1.2 Smart Phones:	60
3.6.1.3 Phone USB	61
3.6.2 Software Tools.....	61
3.6.2.1 Eclipse.....	61
3.6.2.2 NetBeans	61
3.7 Chapter Summary.....	62
CHAPTER 4 SYSTEM IMPLEMENTATION AND EVALUATION	
4.1 Introduction.....	63
4.2 The Proposed System Design	63
4.3 System Operation.....	65
4.3.1 Creating Account.....	65
4.3.2 User Account Activation.....	67
4.3.3 Accessing Government Data	68
4.4 Results Interface.....	70
4.5 Hybrid technique performance using digital envelope on Smartphones.....	75
4.6 Results of NTRU and AES performance on Smartphones.....	77
4.8 A note on relative performance of algorithms on mobile devices compared to PC.....	79
4.8.1 NTRU Activation process (Encryption) on PC	79
4.8.2 AES access activity on PC	80

4.9 Chapter Summary.....	82
CHAPTER 5_CONCLUSION AND FUTURE WORK	
5.1 Research Contributions	83
5.2 Research Limitations.....	85
5.3 Summary of Research Findings.....	86
5.4 Direction of Future Works.....	86
REFERENCES.....	88