RSA PERFORMANCE EVALUATION FOR PRIVACY PRESERVING SCHEME
IN INTERNET OF THINGS.

BAHAREH MALEKI ALAVI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013
This project report is dedicated to my family especially my mom and dad for their endless support and encouragement.
ACKNOWLEDGEMENT

First praise and thanks are for Allah who is guiding us continually and all the life especially for this graduating section. The one who is always available and hear our speaking then show the suitable way to human based on their requirements.

Upon the successful completion of this project, I would like to express my sincere thanks to Dr. Mohammad Abdur Razzaque, my supervisor, for his encouragement, guidance and advices. Thanks for all the time he spent for me along this project and showed me the way of researching.

My sincere appreciation also goes to Dr. Anazida Zainal who patiently listen to me and guided me where I need. At the end, my utmost thanks go to my parents and my whole family which are not near me but encourage me from my country in the whole graduating path specifically for this project and gave me the strength of face the different challenges.
ABSTRACT

A worldwide network of interconnected objects which are uniquely addressable, based on standard communication protocols is called: Internet of Things (IOT). As the Internet of Things is a large field with diverse technologies used there is a categorization of components including: Communication, sensors/RFID sensors, actuators, storage, devices, processing, localization and Tracking that each component has its own special problems of security which might be happened. The major factor which plays an important role in the future Internet of Things is Privacy. The protection of data and privacy of users is one of the key challenges in Internet of Things. Lack of confidence about privacy is one of the driving factors in the success of intelligent collaboration of miniaturized sensors. So it is needed to identify an applicable mechanism of privacy in internet of things. As RFID tags identify unique items and RFID market is growing fast and also RFID tags posing an important role in Internet of Things, various mechanisms exist for privacy. In this project evaluation of existing mechanisms in RFIDs has been considered and enhanced mechanism selected in this area. By using the Montgomery reduction for implementing the RSA algorithm and combing by hybrid method in multiplication, improvement in performance is achieved based on clock cycle counts.
ABSTRAK

Dalam satu rangkaian seluruh dunia antara objek yang saling berhubung di mana ianya dicapai dengan alamat yang unik, berdasarkan standard protokol komunikasi yang dipanggil: Perkara Internet (IOT). Diketahui bahawa Perkara Internet adalah satu bidang yang besar dengan pelbagai teknologi yang digunakan, setiap komponen mempunyai masalah keselamatan tersendiri yang mungkin berlaku. Faktor utama yang memainkan peran penting dalam Perkara Internet pada masa hadapan adalah Peribadi (Privasi). Perlindungan terhadap data dan privasi pengguna adalah salah satu cabaran utama dalam Perkara Internet. Kekurangan dalam keyakinan terhadap privasi adalah salah satu faktor yang mendorong kejayaan dalam kerjasama pintar terhadap sensor miniatur. Jadi ia diperlukan untuk mengenal pasti satu mekanisme berkaitan privasi dalam Perkara Internet. Diketahui bahawa tag RFID boleh mengenal pasti sesuatu barang yang unik dan pasaran RFID berkembang pesat dan tag RFID juga memainkan peranan penting dalam Perkara Internet, wujud pelbagai mekanisme untuk privasi. Dalam kes ini, penilaian projek terhadap mekanisme sedia ada dalam RFIDs telah diguna pakai dan mekanisme yang dipilih dipertingkatkan dalam bidang ini. Dengan menggunakan pengurangan Montgomery untuk melaksanakan algoritma RSA dan mengintegrasikan melalui kaedah hibrid dalam pendaraban, peningkatan dalam prestasi dicapai pada kiraan kitaran jam.
CHAPTER 1

INTRODUCTION

1.1 Introduction

In this chapter, a description of the background and statement of the problem for this project are presented. In continue, objectives of this project are illustrated. Then description for the scope and significance for this project is determined in separate sections clearly.

1.2 Background of the Study

In the first days of creation of ARPANET no one knew that this combination of four existing nodes will grow in this speed and at least such a great interconnected networks in all over the world will be developed. Networks which will be in high performance with capability of self-organizing in the future. As a statistic view, the population of people who use this World Wide Web network is increasing till they are now approximately 1.5 billion which is about 20% of the whole population of the world. Several reasons such as huge amount of people and end users all over the world, extent of various types of networks, production of advanced systems and devices with high computational performance and less amount of energy consumption bring out different styles of living which are new and lead us to have a
special trend to accept the concept which is addressed as Internet Of Things. The study in this field has started from 2006 and still continues because of need to connect smart manufactures and devices to each other. With development of smart manufactures, these smart objects can connect to the Internet and they can be remotely configured and updated. These benefits can be used in houses, offices, health care centers, transportation, animal protection, shopping centers and so on (Wang et al. 2010).

As a result of connecting different objects to each other to obtain the Internet of Things (IOT), several techniques may be used as enablers of IOT such as RFIDs. Radio Frequency Identification technology with specific capabilities will be used as one of the backbones of IOT. Due to low consumption of energy, low price and easy to implementation, use of RFID as an alternative to barcode is increasing and will continue in future. In the past RFID was only used in Retail and logistics but nowadays RFID tags are used in various positions such as payment services and transportations and in each position where an ID as identification makes a big role. Inside these interconnected networks beside sensors and different technologies, several issues will be faced. One of the most important issues because of the nature of IOT and existence of communication in such situation is security and privacy problem. If people do not get enough confidence about their personal information in such environment with new technologies they will not move forward to this new technology (Mayer 2009b; Leusse et al. 2009).

A RFID system consists of RFID tag, RFID reader and a back end server. As RFID tag covers identification of unique devices, privacy issue will be raised. That’s why it is important to make an effort to solve privacy problem and prepare suitable security first before or in parallel of implementation to adapt people with IOT. There are several mechanisms of protecting security of RFID systems that we can categorize them in two big parts as physical mechanisms such as kill codes, Faraday cage and blocker tag and second cryptographic methods which are known as Randomized Hash-Lock Protocol and Hash Chain based Protocols. Several studies have been done in this area and also some schemes have been proposed which have
their own attributes (Mayer 2009b; Anon n.d, 2009). These works require further investigation for better improvements.

1.3 Statement of the Problem

Internet of Things means “a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols.” As mentioned before IOT includes several technologies and is a wide area, There are a categorize set of components such as: Communication, sensors/RFID sensors, actuators, storage, devices, processing, localization and tracking. Each component may have its specific issue of security but as IOT penetrates our daily life things the most important problems is privacy which has been shown in the study. (Mayer 2009b) There are several types of attitude to RFID’s world with different aspects. We can categorize studies done in this case to three ways as: technology, law and regulation and management (Tao and Peiran 2010). In the first area for enhancement of algorithms as a result there are several mechanisms for solving security problems.

For adapting people with the future IOT, it is needed to protect data and personal information in each component. Several studies in this area have been done and as a result some security frameworks and schemes have been proposed but it is still an open area because of the span of IOT and security aspects in this environment. So it is necessary to evaluate the existing mechanisms in this area and propose the best one and improve its capabilities (Anon, 2010).

1.4 Purpose of the Study

First purpose of this study is to review the concept of Internet of Things, attributes and its role in the future life and its components. Then it is concentrated on
RFID, one of enablers of IOT and study and evaluating their security mechanisms which provide privacy is done. In continue, it is aimed to improve the existing situation of privacy in this world to protect important information from probable threats.

1.5 Objectives of the Study

In this project, it is supposed to achieve to some specific objectives which are mentioned as below:

- To study IOT and identify RFIDs and privacy issues in this field.
- To analyze current mechanisms of solving the privacy issues in RFID in the IOT perspective to propose an enhanced mechanism.
- To introduce the optimized methods of implementing RSA algorithm using in that mechanism and compare the results for improving the performance.

1.6 Research Questions

Some important questions may be asked in this field as an Internet Of Things perspective which are like below:

- What are the main roles of security problems in success of implementation of IOT? Do they have any specific limitations?
- Why protect of personal information of end users and tracking of their activities which are using IOT, is so important?
• Will the proposed security mechanism cover all the existing gap and vulnerabilities? How much is the proposed mechanism reliable and confidence due evaluation?

1.7 Significance of the Study

The importance of this study is related to significance of Internet OF Things in the future life, where each object may connect to network and also to Internet. Therefore they can communicate with each other and needed information is gathered easily. As a result, it is viable to having control on objects remotely which may have important role in logistics, transportation, medical centers and drugs, shopping centers and specific smart objects for example at houses. But in this situation protecting personal information of people or objects from probable vulnerabilities will be so important. That is why having suitable privacy mechanisms for this critical situation is so needed.

1.8 Scope of the Study

In this project evaluation of the privacy issues in existing component of IOT is done and it is concentrated specifically on RFID as an enabler of IOT. The existing mechanisms of protecting privacy issues of RFID in the world of IOT is evaluated and then for improving the performance in the specific scheme, optimized methods for implementing RSA algorithm are compared.
1.9 Summary

In this chapter, the introduction in the problem statement and the objectives of this project is introduced then description in the significance of this project is done clearly based on the projects scopes and research questions.

Inside chapter 2, the literature review of this project is described then the research methodology of whole project is introduced in chapter 3. The selected scheme for privacy preserving and its different functionality steps are described in chapter 4. In continue the optimized methods for implementing the RSA encryption and also some obtained results are compared in chapter 5. The achievements of whole project and also limitations of this project are presented in chapter 6.
REFERENCES


J. Anon, 2010, An architecture based on Internet of Things to support mobility and security in medical environments. *IEEE consumer communication and networking conference*


Corporation, H., IMPLEMENTATIONS OF MONTGOMERY MULTIPLICATION ALGORITHMS IN MACHINE.


TABLE OF CONTENTS

CHAPTER TITLE PAGE

DECLARATION ii
DEDICATION iii
ACKNOWLEDGEMENT iv
ABSTRACT v
ABSTRAK vi
TABLE OF CONTENT vii
LIST OF TABLES xi
LIST OF FIGURES xii

1 INTRODUCTION
1.1 Introduction 1
1.2 Background Of the study 1
1.3 Statement of the problem 3
1.4 Purpose of the study 3
1.5 Objectives of the Study 4
1.6 Research Questions 4
1.7 Significance Of the Study 5
1.8 Scope of the Study 5
1.9 Summary 6

2 LITERATURE REVIEW
2.1 Introduction 7
2.2 Internet of Things (IOT) 7
<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1 Enablers of IOT</td>
</tr>
<tr>
<td>2.2.2 Architecture of IOT</td>
</tr>
<tr>
<td>2.2.3 The development of IOT</td>
</tr>
<tr>
<td>2.2.4 Categorization of components and sensitivity</td>
</tr>
<tr>
<td>2.3 RFID technology</td>
</tr>
<tr>
<td>2.4 The Use of RFID and IOT</td>
</tr>
<tr>
<td>2.5 RFID Attacks and Countermeasures</td>
</tr>
<tr>
<td>2.6 Privacy Issues</td>
</tr>
<tr>
<td>2.6.1 Preference-Based Privacy Protection Mechanism</td>
</tr>
<tr>
<td>2.6.2 A Cross Layer framework for privacy enhancement in RFID</td>
</tr>
<tr>
<td>2.6.3 Three recent approaches</td>
</tr>
<tr>
<td>2.6.4 A Hybrid approach for privacy preserving RFID tags</td>
</tr>
<tr>
<td>2.7 Basic Multiplication Techniques</td>
</tr>
<tr>
<td>2.7.1 Schoolbook method</td>
</tr>
<tr>
<td>2.7.2 Comba’s method</td>
</tr>
<tr>
<td>2.7.3 Karatsuba’s method</td>
</tr>
<tr>
<td>2.7.4 Hybrid Multiplication</td>
</tr>
<tr>
<td>2.8 Montgomery modular Multiplication</td>
</tr>
<tr>
<td>2.9 Summary</td>
</tr>
</tbody>
</table>

3 RESEARCH METHODOLOGY

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Introduction</td>
</tr>
<tr>
<td>3.2 Research Workflow</td>
</tr>
<tr>
<td>3.3 Respondents of the Study</td>
</tr>
<tr>
<td>3.4 Research Instruments Used</td>
</tr>
<tr>
<td>3.5 Data Analysis</td>
</tr>
<tr>
<td>3.6 Summary</td>
</tr>
</tbody>
</table>
# Analysis and Design

4.1 Introduction 29

4.2 RT scheme steps 29

4.3 Security analysis of RT scheme 29

4.4 Efficiency 32

4.5 Encryption method 34

4.6 Improve the Encryption implementation 34

4.7 Summary 34

# Implementation Method Evaluation

5.1 Introduction 36

5.2 Preliminaries 37

5.3 Modular Exponentiation 38

5.3.1 Flow chart of m-ary algorithm 39

5.4 Liu et al ‘s implementation method 40

5.4.1 Improved hybrid method 40

5.4.2 Hybrid Montgomery Multiplication 43

5.5 Wang et al ‘s implementation method 44

5.6 Wander et al ‘s implementation method 44

5.7 Performance evaluation of RSA algorithm implementation 45

5.8 Summary 46

# Discussion & Conclusion

6.1 Introduction 48

6.2 Discussion 48

6.3 Achievements 49

6.4 Limitations and Future works 49

6.5 Conclusion 50
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Comparison of Instruction counts on the ATmega128</td>
<td>42</td>
</tr>
<tr>
<td>5.2</td>
<td>Performance of 1024-Bit RSA implementation</td>
<td>46</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Structure of a system in IOT perspective</td>
<td>11</td>
</tr>
<tr>
<td>2.2</td>
<td>Sensitivity of each component in IOT against security</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>The comparison between Hybrid scheme (RT) and other methods</td>
<td>19</td>
</tr>
<tr>
<td>2.4</td>
<td>Montgomery reduction algorithm</td>
<td>23</td>
</tr>
<tr>
<td>3.1</td>
<td>Workflow of process</td>
<td>25</td>
</tr>
<tr>
<td>4.1</td>
<td>Protocol setup phase</td>
<td>30</td>
</tr>
<tr>
<td>4.2</td>
<td>Protocol execution phase</td>
<td>31</td>
</tr>
<tr>
<td>5.1</td>
<td>M-ary method algorithm</td>
<td>38</td>
</tr>
<tr>
<td>5.2</td>
<td>The flowchart of m-ary algorithm</td>
<td>39</td>
</tr>
<tr>
<td>5.3</td>
<td>Register allocation between Original and new hybrid method</td>
<td>41</td>
</tr>
<tr>
<td>5.4</td>
<td>Comparison chart for instruction count between original and new hybrid method</td>
<td>42</td>
</tr>
<tr>
<td>5.5</td>
<td>HSOS integration view</td>
<td>43</td>
</tr>
<tr>
<td>5.6</td>
<td>The comparison chart based on clock cycle count</td>
<td>46</td>
</tr>
</tbody>
</table>