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 peranan 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 miniaturi. Jadi ia diperlukan untuk mengenal pasti satu mekanisme berkenaan 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.