USER-DEVICE AUTHENTICATION MODEL WITH DIGITAL CERTIFICATE FOR SMARTPHONE USER

SAKIINAH BINTI ALTAF HUSSAIN

UNIVERSITI SAINS ISLAM MALAYSIA

USER-DEVICE AUTHENTICATION MODEL WITH DIGITAL CERTIFICATE FOR SMARTPHONE USER

Sakiinah binti Altaf Hussain

Thesis submitted in partial fulfillment for the degree of
MASTER OF SCIENCE

UNIVERSITI SAINS ISLAM MALAYSIA

October 2024

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 2nd October 2024 Signature:

Name: Sakiinah binti Altaf Hussain

Matric No: 3201278

Address: [redacted]

Georgetown, Pulau Pinang

ACKNOWLEDGEMENTS

Praise be upon Allah the Most Gracious Most Merciful for His blessing and give me the strength to endure the challenges while completing this thesis entitled "USER-DEVICE AUTHENTICATION MODEL WITH DIGITAL CERTIFICATE FOR SMARTPHONE USER" for the master thesis report.

I would like to thank everyone who has contributed to the successful completion of this thesis. Firstly, I would like to express my deepest sincerity gratitude to my researcher supervisor, Prof. Madya Dr. Azni Haslizan Ab. Halim and co-supervisor, Prof. Madya Dr. Najwa Hayaati Mohd Alwi for their valuable advice, guidance, and their enormous patience throughout the proposal of the authentication model and written thesis.

Besides, my sincere appreciation goes to my parents and family, especially to Altaf Hussain bin Shri Abdul Aziz and Serah Banu binti Sadar Mohd as well as to my siblings for their full support and prayers for my success. I also would like to dedicate my special thanks to my friends and my seniors who contributed their help in completing this thesis.

Thank you. May Allah bless us.

ABSTRAK

Telefon pintar adalah sebahagian daripada Internet Benda, menghubungkan objek harian seperti rumah, hospital dan banyak lagi ke Internet dan menyediakan platform untuk komunikasi. Untuk melindungi data pengguna daripada capaian yang tidak dibenarkan, adalah penting untuk menggabungkan teknologi kriptografi ke dalam aplikasi telefon pintar untuk memastikan data yang dihantar melalui penghantaran wayarles selamat dan dikongsi hanya dengan peranti yang dimaksudkan. Ini disebabkan oleh peningkatan pesat kecurian identiti, pelanggaran data dan serangan yang disebabkan oleh skim pengesahan yang lemah, pengurusan kata laluan yang lemah dan pancingan data. Untuk memerangi ancaman ini, adalah penting untuk memasukkan aplikasi pengesahan selamat ke dalam telefon pintar. Tesis ini bertujuan untuk membangunkan model pengesahan yang menggabungkan penggunaan sijil digital dan kunci rahsia untuk menyulitkan dan menyahsulit data. Model ini direka bentuk untuk membolehkan pengguna telefon pintar mengesahkan diri mereka dengan sijil digital, membolehkan mereka mengakses aplikasi daripada peranti pengguna. Algoritma Rivest–Shamir–Adleman (RSA) digunakan untuk menjana kunci, dan sijil digital kemudiannya dikeluarkan untuk mengesahkan identiti pengguna dan identiti peranti. Matlamat tesis adalah untuk menyiasat keperluan pengesahan untuk pengguna telefon pintar, membangunkan model pengesahan untuk pengguna telefon pintar, dan menilai keupayaan untuk mengesahkan pengguna dan peranti dalam pengguna telefon pintar. Untuk mencapai objektif, pendekatan utama adalah untuk menyemak literatur tentang keperluan pengesahan untuk peranti telefon pintar, yang membawa kepada pelaksanaan sijil digital untuk pengesahan pengguna dan peranti. Model pengesahan pengguna dan peranti, yang melaksanakan sijil digital untuk pengguna telefon pintar, terdiri daripada tiga fasa: Fasa Pendaftaran, Fasa Sijil Digital dan Fasa Pengesahan. Untuk mengesahkan model, dua kaedah digunakan. Pertama, ujian kualitatif dijalankan dengan menjemput ulasan pakar untuk memberikan pendapat mereka tentang model dan semua fasa, serta menjawab soal selidik. Kedua, data matematik digunakan untuk mengesahkan aliran model, menggunakan formula yang terkandung di dalamnya. Model yang dicadangkan boleh berfungsi sebagai rujukan untuk aplikasi telefon pintar, mengesahkan kedua-dua pengguna dan peranti bersama-sama untuk pengesahan yang dipertingkatkan yang boleh melindungi data daripada pengguna yang tidak dibenarkan dan berfungsi sebagai batu loncatan untuk pelaksanaan keselamatan untuk aplikasi dalam telefon pintar.

Kata kunci: kriptografi, pengesahan, pengesahan, algoritma RSA

ABSTRACT

Smartphones are an integral part of the Internet of Things, connecting everyday objects such as homes, hospitals, and more to the internet and providing a platform for communication. To protect user data from unauthorized access, it is essential to incorporate cryptography technology into smartphone applications to ensure that data transmitted via wireless transmission is secure and shared only with the intended devices. This is due to the rapid rise of identity theft, data breaches, and attacks caused by weak authentication schemes, poor password management, and phishing. To combat these threats, it is important to incorporate secure authentication applications into smartphones. This thesis seeks to develop an authentication model that combines the use of a digital certificate and a secret key to encrypt and decrypt data. This model is designed to enable smartphone users to authenticate themselves with a digital certificate, allowing them to access applications from the user's device. The Rivest–Shamir–Adleman (RSA) algorithm is used to generate the key, and the digital certificate is then issued to verify the user's identity and the device's identity. The proposed model using RSA algorithm because RSA signature generation is essentially the process of raising a big integer to the power of the exponent of the private key. Because the RSA private keys may be selected with tiny exponents, which speeds up the signature creation process, this procedure is efficient. The thesis aims to investigate the authentication requirements for smartphone users, develop an authentication model for smartphone users, and evaluate the ability to authenticate users and devices in smartphone users. To achieve the objectives, the primary approach is to review the literature on authentication needs for smartphone devices, which leads to the implementation of digital certificates for both user and device authentication. The user and device authentication model, which implements digital certificates for smartphone users, consists of three phases: Registration Phase, Digital Certificate Phase, and Authentication Phase. To validate the model, two methods are employed. Firstly, qualitative testing is conducted by inviting expert reviews to provide their opinion on the model and all phases, as well as responding to questionnaires. Secondly, mathematical data is used to verify the flow of the model, using the formula contained therein. The model proposed can serve as a reference for smartphone applications, authenticating both users and devices together for enhanced verification that can protect data from unauthorized users and serve as a springboard for the implementation of security for applications in smartphones.

Keywords: cryptography, authentication, validation, RSA algorithm

املخص

تعد الهواتف الذكية جزءًا لا يتجزأ من إنترنت الأشياء، حيث تربط الأشياء اليومية مثل المنازل والمستشفيات وغيرها بالإنترنت وتوفر منصة للاتصال .لحماية بيانات المستخدم من الوصول غير المصرح به، من الضروري دمج تقنية التشفير في تطبيقات الهواتف الذكية لضمان أن البيانات المنقولة عبر النقل اللاسلكي آمنة ومشتركة فقط مع الأجهزة المقصودة .ويرجع ذلك إلى الارتفاع السريع في سرقة الهوية وانتهاكات البيانات والهجمات الناجمة عن أنظمة المصادقة الضعيفة وسوء إدارة كلمات المرور والتصيد الاحتيالي .ولمواجهة هذه التهديدات، من المهم دمج تطبيقات المصادقة الآمنة في الهواتف الذكية .تسعى هذه الأطروحة إلى تطوير نموذج مصادقة يجمع بين استخدام الشهادة الرقمية والمفتاح السري لتشفير وفك تشفير البيانات .تم تصميم هذا النموذج لتمكين مستخدمي الهواتف الذكية من مصادقة أنفسهم بشهادة رقمية، مما يسمح لهم بالوصول إلى التطبيقات من جهاز المستخدم .يتم استخدام خوارزمية Rivest–Shamir–Adleman (RSA) لإنشاء المفتاح، ثم يتم إصدار الشهادة الرقمية للتحقق من هوية المستخدم وهوية الجهاز .الهدف من هذه الأطروحة هو دراسة متطلبات المصادقة لمستخدمي الهواتف الذكية، وتطوير نموذج مصادقة لمستخدمي الهواتف الذكية، وتقييم القدرة على مصادقة المستخدمين والأجهزة لدى مستخدمي الهواتف الذكية .من أجل تحقيق الأهداف، يتمثل النهج الأساسي في مراجعة الأدبيات المتعلقة باحتياجات المصادقة لأجهزة الهواتف الذكية، مما يؤدي إلى تنفيذ الشهادات الرقمية لكل من مصادقة المستخدم والجهاز. يتكون نموذج مصادقة المستخدم والجهاز، الذي يطبق الشهادات الرقمية لمستخدمي الهواتف الذكية، من ثلاث مراحل :مرحلة التسجيل، ومرحلة الشهادة الرقمية، ومرحلة المصادقة .للتحقق من صحة النموذج، يتم استخدام طريقتين .أولاً، يتم إجراء الاختبار النوعي من خلال دعوة مراجعات الخبراء لإبداء رأيهم حول النموذج وجميع مراحله، بالإضافة إلى الرد على الاستبيانات .ثانيًا، يتم استخدام البيانات الرياضية للتحقق من تدفق النموذج باستخدام الصيغة الواردة فيها .يمكن أن يكون النموذج المقترح بمثابة مرجع لتطبيقات الهواتف الذكية، حيث يقوم بمصادقة كل من المستخدمين والأجهزة معًا من أجل التحقق المعزز الذي يمكن أن يحمي البيانات من المستخدمين غير المصرح لهم ويكون بمثابة نقطة انطلاق لتنفيذ الأمان للتطبيقات في الهواتف الذكية.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figures **Page**

LIST OF APPENDICES

LIST OF SYMBOLS

P	Plaintext
C	Ciphertext
K	Key
EK	Encryption Algorithm Contains Key
$EK{-}1$	Decryption Algorithm Contains Key
SMS	Short Message Services
SIM	Subscriber Identity Module
PIN	Personal Identification Number
TAC	Transaction Authorization Code
CA	Certificate Authority
VPN	Virtual Private Networks
p	First Prime Number
q	Second Prime Number
n	Value by Multiplying P and Q
Φ(n)	Euler's Totient
E	Public Exponential
D	Private Key
Kpub(u)	Public Key User
Kpub(d)	Public Key Device
Kpub(ca)	Public Key Certificate Authority
Kpr(u)	Private Key User
Kpr(d)	Private Key Device
Kpr(ca)	Private Key Certificate Authority
Uid	User ID
Up	User's Password
Din	Device IMEI Number
Upn	User's Phone Number
Sa(U)	Signature User
Sa(U)'	Verification Signature User
Sa(D)	Signature Device
Sa(D)'	Verification Signature Device
Cert(U)	Certificate User
Cert(D)	Certificate Device
α	Cronbach's Alpha
k	Number of Questionnaires
s_y^2	Variance of the Total Scores of Each Question
s_i^2	Variance of Each Individual Question.
(n,e)	Public Key
(n,d)	Private Key

LIST OF EQUATIONS

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
AMOLED	Active-Matrix Organic Light-Emitting Diode.
ASCII	American Standard Code for Information Interchange
BDS	Basic Digital Signature
CA	Certificate Authority
CPU	Central Processing Unit
CRL	Certificate Revocation List
CS	Control Server
CSS	Cascading Style Sheet
DHKE	Diffie-Hellman Key Exchange
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
HTTPS	Hypertext Transfer Protocol Secure
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
LCD	Liquid Crystal Display
MCMC	Malaysian Communications and Multimedia Commission
MIM	Man-in-the-Middle
NAND	Not-And
OLED	Organic Light-Emitting Diode
OTP	One-time Password
PDF	Portable Document Format
PHP	Hypertext Preprocessor
PII	Personal Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature
QR	Quick Response code
RAM	Random Access Memory
RFID	Radio-Frequency Identification
SES	Simple Electronics Signature
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Services
SQL	Structured Query Language
SSH	Secure Socket Shell

SSC	Shamir Secret Share
SSL/TLS	Secure Socket Layer/Transport Layer Security
TAC	Transaction Authorization Code
TDR	Transient data storage
UML	Unified Modelling Language
URL	Uniform Resource Locator