CLOUD COMPUTING THREE-FACTOR USER AUTHENTICATION FRAMEWORK AND PROTOCOLS FOR TELECARE MEDICAL INFORMATION SYSTEM

ZEESHAN SIDDIQUI

UNIVERSITI TEKNOLOGI MALAYSIA

CLOUD COMPUTING THREE-FACTOR USER AUTHENTICATION FRAMEWORK AND PROTOCOLS FOR TELECARE MEDICAL INFORMATION SYSTEM

ZEESHAN SIDDIQUI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

SEPTEMBER 2015

DEDICATION

I dedicate this study to my affectionate and beloved Prophet Muhammad (صلى الله عليه وسلم), his Companions (رضى الله عنهم ورضوا عنه) and those who followed him (رحمة الله عليه). Additionally, I dedicate this study to my compassionate parents, beloved wife and enthusiastic kids for their persistent support, zeal and love.

ACKNOWLEDGEMENT

All praises and commendations goes to the Almighty Allah (سبحانه و تعالى) for accepting my motivation, enthusiasm and passion to complete this astonishing study and to achieve a remarkable goal. Supreme blessings and peace of the Almighty Allah be upon Prophet Muhammad (صلى الله عليه وسلم), his Companions (رضى الله عنهم ورضوا عنه) and those how followed them. I am wholeheartedly thankful to my supervisor Professor Dr. Abdul Hanan Abdullah, for his kind and humble support towards my continuous and intense research work. I am among those prosperous persons who were extremely fortunate to have such a brilliant individual as an advisor for complete guidance at each and every stage of this study. I am passionately an admirer a devotee of my co-external supervisors Dr. Muhammad Khurram Khan and Professor Abdullah Alghamdi for providing me their friendly and persistent support throughout my studies. I am so much grateful to all of my advisors for delivering their brilliance and genius to make a dream come true. A million thanks to Dr. Saqib Ali and Imran Hayat for providing their excellence, quality and support during my study. Additionally, I am thankful to my institute, faculty, staff and colleagues for providing me such a remarkable environment where I can express my abilities and deliver excellence. A sincere, explicit and emphatic word of thanks to my mother and father, my loving wife and my lively kids for their love, patience, support, prayers and understanding all the way through my study. I am short of words for their support, as without their encouragement and reassurance, this success was not achievable.

Zeeshan Siddiqui, Universiti Teknologi Malaysia

ABSTRACT

The Telecare Medical Information System (TMIS) provides a set of different medical services to patients and medical practitioners. The patients and medical practitioners can easily connect to the services remotely from their own premises, whereas, medical practitioners can observe the wellbeing of their patients remotely. There are several studies carried out to securely authenticate a remote user to use the TMIS facility more securely. Researchers have proposed several Smartcard authentication protocols for TMIS systems while addressing a number of authentication attacks along with performance issues. However, current TMIS authentication mechanism is highly vulnerable to a number of authentication attacks. Therefore lacks a completely secure, authentic and validated authentication framework. The primary objective of this study is to propose a secure Cloud Computing Three Factor user authentication framework and protocols for TMIS facility. To accomplish this, the authentication framework is supported by TMIS Service Cataloguing and Initialization protocol and TMIS Service Stimulation and Reset Protocol. The framework and protocols are verified using Burrows Abadi Needham logic standard and validated using Scyther authentication testing. The performance is judged using Profiler Analysis. The security and performance analysis has proved that the design and developed framework and protocols are highly resilient to classical and modern authentication attacks while maintaining higher level of security during the complete authentication process. The authentication analysis has proved that the proposed work has delivered a verifiable and validated security framework and protocols for TMIS facility.

ABSTRAK

Sistem Maklumat Perubatan Telepenjagaan (TMIS) menyediakan satu set perkhidmatan perubatan yang berbeza untuk pesakit dan pengamal perubatan. Para pesakit boleh menyambung kepada perkhidmatan jarak jauh dari premis mereka sendiri, manakala pengamal perubatan dapat memerhatikan kesihatan pesakit mereka dari jauh. Terdapat beberapa kajian yang dijalankan bagi mengesahkan penggunaan kemudahan TMIS dengan lebih selamat. Para penyelidik telah mencadangkan beberapa protokol pengesahan Kad Pintar berasaskan sistem TMIS bagi menangani beberapa serangan pengesahan bersama-sama dengan isu-isu prestasi. Walau bagaimanapun, mekanisma pengesahan TMIS semasa adalah sangat terdedah kepada beberapa serangan pengesahan. Oleh itu ianya tidak mempunyai rangka kerja pengesahan yang benar-benar selamat, tulen dan disahkan. Objektif utama kajian ini adalah untuk mencadangkan rangka kerja pengesahan pengguna Pengkomputeran Awan Tiga Faktor dan protokol yang selamat untuk kemudahan TMIS. Untuk mencapai objektif ini, rangka kerja pengesahan disokong oleh TMIS Perkhidmatan Pengkatalogan dan Permulaan protokol dan TMIS Perkhidmatan Rangsangan dan Reset Protocol. Rangka kerja dan protokol ditentusahkan menggunakan piawai logik Burrows Abadi Needham dan disahkan menggunakan ujian pengesahan Scyther. Prestasi dinilai menggunakan Analisis Pemprofile. Keselamatan dan prestasi analisis telah membuktikan bahawa reka bentuk dan kemajuan rangka kerja dan protokol sangat berdaya tahan kepada serangan pengesahan klasik dan moden di samping mengekalkan tahap keselamatan yang tinggi semasa proses pengesahan yang lengkap. Analisis pengesahan telah membuktikan bahawa kerja yang dicadangkan itu menyampaikan rangka kerja keselamatan yang telah dikenalpasti dan disahkan dan protokol untuk kemudahan TMIS.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

1FA	-	First Factor Authentication
2FA	-	Two Factor Authentication
3FA	-	Three Factor Authentication
1G	-	First Generation
2G	-	Second Generation
3G	-	Third Generation
3DES	-	Triple Data Encryption Standard
2D	-	Two Dimensional
4FA	-	Fourth Factor of Authentication
AHP	-	Analytical Hierarchy Process
ATM	-	Automated Teller Machine
AFSCC	-	Authentication Framework using Smartphone on Cloud Computing
AD	-	Alzheimer's disease
AES	-	Advance Encryption Standard
BAN	-	Burrows Abadi Needham
CC	-	Cloud Computing
CoSE	-	Cloud Secure Element
CPU	-	Central Processing Unit
DSS	-	Decision Support System
DLP	-	Discrete Logarithms Problem
DoS	-	Denial of Service
DES	-	Data Encryption Standard
DSP	-	Digital Signal Processing
DFT	-	Discreet Fourier Transform
DLL	-	Dynamic Link Library
DB	-	Database

ECG	-	Electrocardiography
EIS	-	Enterprise Information System
ESB	-	Enterprise Service Bus
EE	-	External Event
FA	-	Forgery Attack
FR	-	Frame Rate
FFT	-	Fast Fourier Transformation
FFIEC	-	Federal Financial Institution Examination Council
GPS	-	Global Positioning System
HTTPS	-	Hyper Text Transport Protocol Secure
IDM	-	Identity Management
IMSI	-	International Mobile Subscriber Identity
IMEI	-	International Mobile Station Equipment Identity
IMS	-	IP Multimedia Subsystem
IAAS	-	Infrastructure as a Service
ISO	-	International Organization of Standardization
IEC	-	International Electro technical Commission
IA	-	Insider Attack
IMI	-	Implementation Issues
IPA	-	Impersonation Attack
K2C	-	Key to Cloud
LUA	-	Least Privilege User Account
LHR	-	Lifetime Health Record
MFA	-	Multifactor Authentication
MOHM	-	Ministry of Health Malaysia
MCDM	-	Multi Criteria Decision Making
MCDA	-	Multi Criteria Decision Analysis
MD5	-	Message Digest Algorithm
MAC	-	Media Access Control
MSP	-	Mobile Service Provider Unit
MSSQL	-	Microsoft Structured Query Language
MAV	-	Mutual Authentication Vulnerability
NFC	-	Near Field Communication

NFCTAN	-	NFC ChipTAN
NGN	-	Next Generation Network
NSR	-	New Service Activation/Registration
NPP	-	Service Password Reset Framework
OTP	-	One Time Password
OMOS	-	Integrated Framework
OS	-	Operating System
OOS	-	Object Oriented Scanning
PCI-DSS	-	Payment Card Industry Data Security Standard
PDS	-	Personal Digital Assistant
P2P	-	Peer-to-Peer
PAAS	-	Platform as a Service
PGA	-	Password Guessing Attack
PAA	-	Privilege Access Attack
PCI	-	Performance Computing Issue
RCAM	-	Resource CAtalog Management
RFID	-	Radio Frequency Identification
SOA	-	Service Oriented Architecture
SHA1	-	Secure Hash Algorithm
SRLM	-	Service Cataloguing and Initialization Protocol
SARM	-	New Service Stimulation and Reset Protocol
SSL	-	Secure Socket Layer
SMCBA	-	Secure Mobile Computing with Biometric Authentication
SDK	-	Software Development Kit
SAAS	-	Software as a Service
SPDL	-	Standard Page Description Language
SGML	-	Standard Generalized Markup Language
SSA	-	Server Spoofing Attack
SA	-	Spyware Attack
SME	-	Small Medium Enterprises
TMIS	-	Telecare Medical Information System
TCP/IP	-	Transport Control Protocol/Internet Protocol

TSCE	-	TMIS Smartphone based Cloud Environment
TSP	-	TMIS Service Provider
URL	-	Universal Resource Locators
UA	-	User/Server Anonymity
USIM	-	Universal Subscriber Identity Module
UAA	-	Unauthorized Access Control
VVI	-	Verification Validation Issue
VMS	-	Virtual Memory System
Web2ID	-	Web to Identification
WSDL	-	Web Service Description/Definition Language
XOR	-	Exclusive OR
XSS	-	Cross Site Scripting Attack

LIST OF SYMBOLS

A_i	-	Registered Authority
A_x	-	Adversary
$\forall$	-	For All (\forall)
β	-	Random Values
CA_i	-	Registered Authority Cloud
E_i	-	Computing Variables
F_i	-	Computing Variables
G_i	-	Computing Variables
H	-	Secret Hash
i	-	Positive Integer
ID_n	-	Identity
${}_1^nV$	-	Session Temporary Variable
m_o	-	Sent OTP Message
M_c	-	MSP Cloud
M_1	-	Message
nS_p	-	New Provider
P_w	-	Registered Password
P_n	-	Updated/New Password
$\mathbf{P} \mid \equiv \mathbf{X}$	-	Message Meaning
$\mathbf{P} \Rightarrow \mathbf{X}$	-	Jurisdiction/Authority
pw	-	Password
pw_{new}	-	New Password
R	-	Request
RB_i	-	Biometrics-image
S_{sk}	-	Session-Keys
$S_c, S(.), h_c$	-	Secure Function of Hash

sk	-	Session Key
S_{mv}	-	Success Message
T_m, T_h	-	Computing Variables for Timestamps
TS_L	-	TMIS Services
uID_i	-	Registered User
uT_s	-	Timestamp
U_i	-	User
V_1, V_2, V_3	-	Computing Variables of Server
V_n	-	Computing Variables
V_s	-	Variable
X	-	Unique Identifier Key
$\oplus$	-	XOR-Operator
♯ (X)	-	Nonce Verification
(x)	-	Freshness
∈	-	Belongs to
⊇	-	Superset of or Equals to
Σ	-	Summation

LIST OF ALGORITHMS

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The modern day health facilities are progressing from outdated paper based environment towards modern and smart digital environments (Pinciroli *et al.*, 2011). Telecare Medical Information Systems (TMIS) is one of those medical systems which facilitate normal user (patient or medical practitioner) to make use of several medical amenities remotely. TMIS was initially developed for older age people, however, this facility has acquired global attention among people of all ages (Megat Ali *et al.*, 2008; Wortmann *et al.*, 2009; Stowe and Harding, 2010). Medical data is considered very sensitive, therefore, secure and authentic TMIS framework is a hot topic from more than a decade. In order to securely authentication a remote user, current TMIS authentication framework is based on Smartcard based Multi-Factor Authentication (MFA), Two Factor Authentication (2FA) and Three Factor Authentication (3FA) authentication protocols (Mishra, 2013). An authentication protocol is comprises of several phases, such as, registration, login, computing, reset and etc. Based on a detailed review, current Smartcard based TMIS authentication protocols have several authentication and verification loopholes, such as, storage of sensitive data within Smartcard, loss of Smartcard, identity theft, eavesdropping and operation interruption (Wu *et al.*, 2012; Zhu, 2012; Yan *et al.*, 2013) .

These issues, in return, have made the current authentication protocols vulnerable to number of authentication attacks, such as, insider attack, impersonation attack, replay attack, online/offline password guessing attack and more (Kim, 2006; He *et al.*, 2013; Kumari *et al.*, 2013; Bin Muhaya, 2014; Khan and Kumari, 2014). In addition to these authentication vulnerabilities, current TMIS authentication framework has number of performance issues, such as, memory usage, hardware support, authentication variable access, application peak time issues etc. (Debiao *et al.*, 2012; Demirkan, 2013; Das and Goswami, 2014). Therefore, this study aims towards pointing out several authentication flaws, along with performance issues within TMIS smartcard based authentication framework.

1.2 Problem Background

While discussing the problem background in this section, a brief discussion of TMIS Architecture is conducted with general TMIS issues and problems (TeleCare, 1987; Sintonen and Immonen, 2013). Moreover, a descriptive debate is carried out to identify the actual TMIS authentication issues addressed in existing studies (Wu *et al.*, 2012; Yan *et al.*, 2013; Tan, 2014). A brief discussion of authentication and performance issues are explained to normalize the propose Cloud Computing (CC) based 3FA authentication framework and protocols which is the main objective of this study along with validation and verification measures (Awasthi and Srivastava, 2013; Das and Goswami, 2014).

1.2.1 TMIS Architecture

In the modern TMIS facility, a patient and a medical practitioner are connected remotely to the TMIS healthcare facility. During the early days, this facility was using First Generation (1G) and Second Generation (2G) resource, like detectors and alarms to monitor patient's health conditions. In case of any activity, resource was detecting and raising alarm to inform the caretakers or community service members of the patient to act accordingly. Due to the global advancements of

information systems, this remote monitoring facility is also transformed into a more advance platform which is widely known as Telehealth. The Telehealth facility is focused on providing more personalized and customized at-home e-health solutions (Brownsell *et al.*, 2008; Stowe and Harding, 2010).

The current TMIS facility make use of modern Third Generation (3G) devices to detect and monitor medical conditions of patients residing at home. This facility is based on agile Service Oriented Architecture (SOA) environment in which patients are connected with the TMIS facility through several wireless devices. These devices are utilized to provide patient complete statistics to their medical consultants and practitioners in order to monitor the health of their patient. With the help of modern-day TMIS facility, a medical consultant can monitor the patient's medical statistics continuously (Megat Ali *et al.*, 2008) as shown in Figure 1.1.

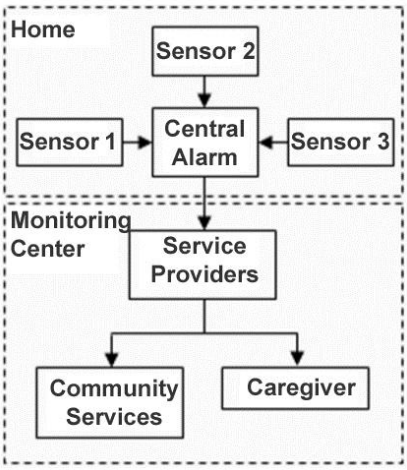

Figure 1.1 The Basic Telecare Framework (Megat Ali *et al.*, 2008)

Originally, this facility was targeting only the elder patients, however, modern TMIS facility is providing a remarkable services to the patients or people of all ages around the globe. Patients and their medical consultants are connected through wireless networks which is further providing interconnection of patient's data. The monitored data is being exchanged remotely between patients and medical consultants. As the patient is not physically present in front of the medical consultant, therefore, whatever data is being transferred and monitored is being treated as it is to measure and propose medical treatments for the remote patient.

Therefore, this information needs to be secured and completely authentic to diagnose and treat patients without any medical error (Megat Ali *et al.*, 2008; Maarop and Win, 2012; Ghani *et al.*, 2013).

Additionally, incurring and installing such a facility at home, require a good amount of finance to be spent. Therefore, there are many factors involved while considering the deployment of TMIS facility at both ends. Factors like, environment, sociality, easiness, customization, cost, hardware, performance, implementation and on top of all, user authentication and security (Megat Ali *et al.*, 2008).

1.2.2 Authentication Protocols and TMIS Vulnerabilities

The purpose of an authentication protocol is to provide a secure data exchange and communication between all the entities of a system using cryptography digital rules (Liang, 2008). An authentication protocol provide assurance of key agreement, undisclosed sharing, non-denial methods and multi-party computation (Kim, 2006). An authentication protocol is based on numerous authentication factors. These authentication factors are recognized by international security standardization bodies (FFIEC, 2006; PCI-DSS, 2008). These factors are,

i. Something User Knows, e.g., username/password. This authentication factor is widely known as First Authentication Factor or 1FA (Coskun and Herley, 2008).
ii. Something User Is, e.g., user biometrics. This authentication factor is widely known as Second Authentication Factor or 2FA (Lakshmiraghavan, 2013).
iii. Something User Has, e.g., a mobile device. This factor is widely known as Third Authentication Factor or 3FA (Fierrez *et al*, 2010).

For a user to get authenticated successfully by utilizing these authentication factors, he/she has to go through a number of authentication phases, namely, registration phase, login phase, computational phase, reset phase and so on (example is shown in Figure 1.2 and 1.3). Modern day authentication protocols, whether implemented within TMIS or outside the domain of Telecare, such as, E-Commerce, are based on the same authentication phases.

There is no major difference in order to authenticate a user utilizing all 3FA(s). The only dissimilarity is the different business rules of that domain. (Guevara-Masis *et al.*, 2004; Hao *et al.*, 2013; He *et al.*, 2013).

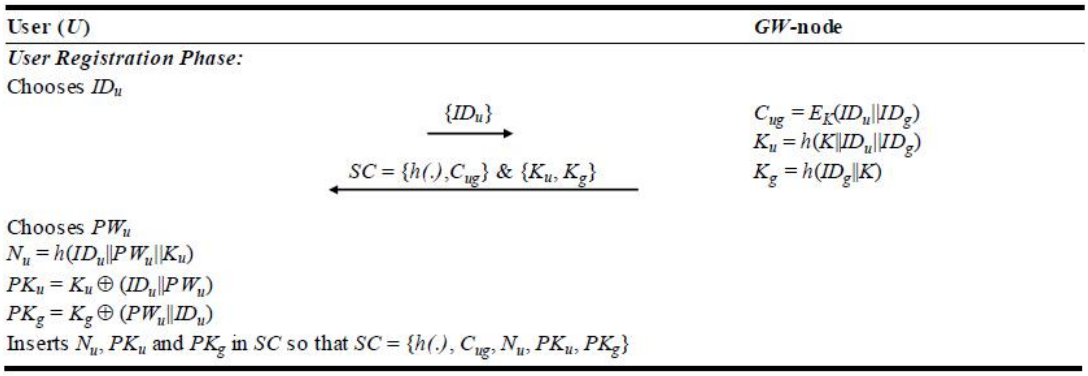

Figure 1.2 Example of Registration Phase (Khan and Kumari, 2013)

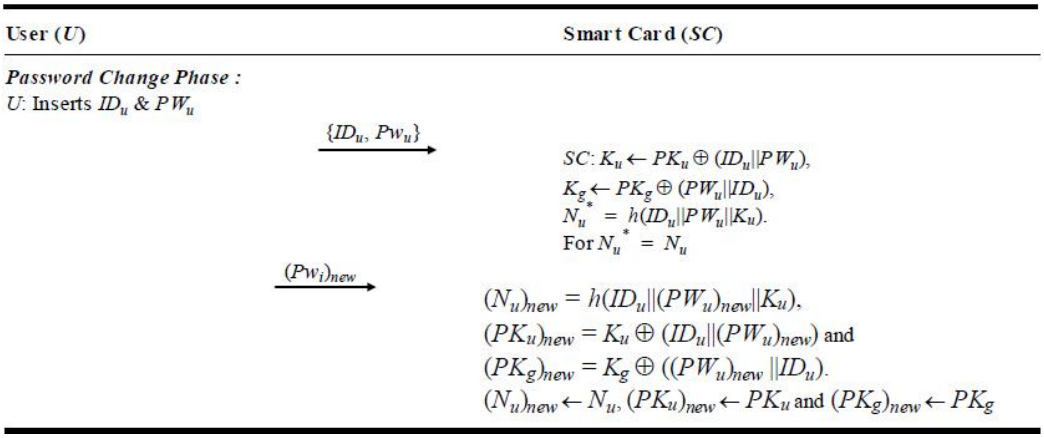

Figure 1.3 Example of Password Change Phase (Khan and Kumari, 2013)

Present TMIS authentication framework is completely dependable on Smartcards. Based on the conducted reviews, current TMIS authentication protocols developed for different authentication phases have several authentication and verification loopholes (Wu *et al.*, 2012; Zhu, 2012; Yan *et al.*, 2013). Such as, Storage of sensitive data within Smartcard, Loss of Smartcard, Identity theft, Eavesdropping, and Operation interruption.

These issues, in return, have made the current authentication protocols vulnerable to number of authentication attacks (Kim, 2006; He *et al.*, 2013; Kumari *et al.*, 2013; Bin Muhaya, 2014; Khan and Kumari, 2014). Such as, Insider Attacks,

Impersonation Attacks, Replay Attacks, Online/Offline Password Guessing Attacks, Parallel Processing Attacks, DOS Attacks, Forgery Attacks, User/Server Anonymity. Expensive proposals of costly TMIS hardware infrastructure is another key factor which is discussed while analysing performance issues (Kim, 2006; He *et al.*, 2013; Kumari *et al.*, 2013).

However, key objective of these studies is to ensure TMIS facility authentication and information security. Most of the aforementioned security threats in the TMIS facility is because of the inconvenient and invalidated implementation of the authentication factors i.e. MFA/2FA/3FA. This is due to the fact that current TMIS authentication studies are not concentrating on developing properly validated and verifiable authentication protocols with respect to the authentication factors involved in it. Most of the studies are relying on manual cryptanalysis of their complete protocol instead of analysing authentication factors by utilizing available logical or automated analysis (Bin Muhaya, 2014; Khan and Kumari, 2014; Mishra *et al.*, 2014a). Absence of this mechanism is making these authentication factors vulnerable to multiple authentication attacks. The most vital and vigorous part of TMIS authentication framework is its secure and robust authentication protocols (Chen *et al.*, 2012). In a normal medical system, patient and medical practitioner's data is sensitive. It gets more sensitive when they are connected through a wireless and remote platform such as a TMIS facility (Chen *et al.*, 2012; Lee, 2013). In any authentication scheme, the security and privacy of the information highly depends on the successful usage of standard factors of authentication (FFIEC, 2006; PCI-DSS, 2008). Like other sectors, healthcare sector has also emerged from 1G to third generation 3G technologies (Kwak *et al.*, 2012; Vassis *et al.*, 2012) and enabled the use of remote healthcare service. These evolvements have made the current TMIS facility vulnerable to number of authentication threats. (Cawley, 2013; Lin, 2013).

1.2.3 Performance, Verification and Validation Issues

Current TMIS studies lacks standardized validation of their authentication protocols by utilizing widely use validation standards and principles such as Burrows Abadi Needham (BAN) Logic, Syverson and Cerbesato (SVO) Logic, ProVerif and

Scyther. (Burrows *et al.*, 1989; Syverson and Cervesato, 2001). These logical standards and principles are built to test and validate the reliability of authentication protocols in terms of message verification, freshness and origin trustworthiness (Burrows *et al.*, 1989; Syverson and Cervesato, 2001)). In order to fill the performance and implementation gap, this study has also pointed out major performance and implementation issues in almost all of the proposed TMIS authentication studies. Such as, Hardware Resources, CPU usage issues, TMIS Application Response Time, Memory Consumption, Excessive use of Variables and Events.

Smartcards are less capable and lacks advance functionalities. Therefore, in order to carry out multiple authentications transactions in hospital, banks or residential premises, a normal person require number of smartcards to carry along. As a result, this has increased the security concerns of theft and loss of smartcards (Cao and Zhai, 2013; Hao *et al.*, 2013; Jiang *et al.*, 2014).

All of these authentication and performance issues outlined above are highly critical in nature and play a vital role during selection and adaptation process of TMIS facility worldwide. Therefore, in this study, designing and development of Cloud Computing based 3FA Authentication Framework and Protocols is presented to ensure the resistance and reliability of the TMIS authentication framework and protocols against number of authentications attacks.

1.2.4 Problem Statement

Current TMIS authentication framework is facing extensive issues such as, lack of authentication details, undefined security steps, less privacy disclosure policies, lack of cloud verification and use of smartphone frameworks without analyzing its security vulnerabilities. Additionally, authentication protocols developed based on these frameworks are vulnerable to loss and theft of smartcards, registration eavesdropping and operation interruptions. These issues have made the existing TMIS authentication protocols vulnerable to insider attack, impersonation attack, reply attack, password guessing attack, parallel processing attack, DoS attack and Forgery attacks.

These vulnerabilities and authentication attacks are due to the continuous utilization of invalidated and fragile use of Smartcards, Smartphone and OTP as 2FA and 3FA. Numerous 2FA and 3FA based authentication protocols were presented and further extended by several researcher. However, almost all of these authentication protocols were having vulnerabilities in their registration, login and reset processes. Major vulnerabilities of these protocols include: storage of sensitive and critical data inside the user Smartcard, loss of identity during login process, multiple errors during protocol execution in login and reset processes and use of plain-text variables during login process. Smartphone based authentication protocols for TMIS were also presented in several studies, however, these studies fail to analyze authentication vulnerabilities and authentication attacks while utilizing a Smartphone as 2FA. Additionally, majority of the protocols were not verified and validated using authentication verification frameworks. Due to these vulnerabilities and attacks, existing TMIS researches fail to provide a complete authentication framework and protocols for TMIS facility.

Therefore, this study has designed and developed a Cloud Computing Three-Factor User Authentication (3FA) Framework and Protocols for TMIS facility to overcome these authentication issues, ambiguities and authentication attacks.

1.2.5 Research Questions

The above problem statement led to the following research questions:

i. How to design and develop Three-Factor Service Cataloguing and Initialization authentication protocol for TMIS in a Cloud Computing environment?
ii. How to design and develop Three-factor Service Stimulation and Reset authentication protocol for TMIS in a Cloud Computing environment?
iii. How to test and validate the authentication of the designed and developed Cloud Computing 3FA TMIS Authentication Framework and Protocols by utilizing BAN Logic and Scyther authentication

testing standards and methods?

1.3 Research Aim

The aim of this thesis is to overcome the current TMIS authentication vulnerabilities and performance issues by designing and developing Cloud Computing Three-Factor User Authentication Framework for Telecare Medical Information System.

1.4 Research Objectives

Based on the above mentioned research questions, following are the research objectives of this thesis:

i. To design and develop Three-Factor Service Cataloguing and Initialization authentication protocol for TMIS in a Cloud Computing environment.
ii. To design and develop Three-Factor Service Stimulation and Reset authentication protocol for TMIS in a Cloud Computing environment.
iii. To test and validate the authentication of the developed Cloud Computing 3FA Authentication Framework and Protocols by utilizing BAN Logic and Scyther testing standards and methods.

1.5 Scope

i. The proposed framework and protocols are based on 1FA/2FA and 3FA authentication factors. These authentication factors are recognized as security standards by different international security standard organizations like FFIEC and PCI DSS. Other factors which

are not yet recognized such as Global Positioning System (GPS) based authentication are not under consideration for this thesis.

ii. This thesis is based on User Authentication Frameworks and Protocols. Biometrics authentication (2FA) can be replaced with other factors of authentication. Therefore, Biometric image processing issues and feature recognition issues are out of the scope of this thesis.

iii. Means of network transformation can be LAN, WAN or any other network. Therefore, specific network protocols, network security issues and network types are not being considered in this thesis.

iv. To satisfy the 3FA requirements, this study has utilized a Smartphone. However, this study is not limited to the use of Smartphone as a 3FA.

v. For concrete analysis in Chapter 2 and in Chapter 6, this study has utilized Analytical Hierarchy Process (AHP) (Siddiqui *et al.*, 2011). AHP compare multiple entities (frameworks/protocols) by assigning weights based on issues and benefits of those entities. To reduce the thickness, final results and charts are only illustrated and discussed.

1.6 Significance of the Study

The current and ongoing TMIS smartcards studies are vulnerable to several authentication loopholes and authentication attacks, including, impersonation attack, replay attack, parallel processing attack, online/offline guessing attacks, insider attack and many other attacks. This study has not just highlighting and further eliminating these authentication vulnerabilities but has also improved other limitations like performance, validation and implementation. Another significance of this study is its tailored used of the mobile phone camera as a biometrics sensor. This capability has also enhanced a normal TMIS user easiness and cost effectiveness by allowing the user to authenticate in the TMIS using his mobile phone camera instead of buying expensive biometric devices. This study can easily be adopted by other sectors and domains, such as, E-Commerce.

1.7 Thesis Organization

The remaining of the thesis is distributed as follows: In Chapter 2, a complete TMIS overview is given by discussing its architecture, capabilities surveys and analysis reports. In this chapter, a detailed and discreet review of previous and current studies are presented that has discussed 3FA authentication protocols and their authentication vulnerabilities. A generalized review is conducted while discussing several smartphone based 2FA/3FA authentication protocols proposed outside the TMIS domain. Chapter 3 presents the research methodology of the proposed authentication framework and protocols. Chapter 4 covers the design, development and implementation of the proposed security and authentication framework and protocols. This chapter also covers, protocol computations along with its algorithms discussion. Authentication verification and validation of the designed and developed authentication framework and protocols is discussed in Chapter 5. The authentication verification is performed using BAN logical postulates along with authentication validation which is performed using Scyther validation of security protocols. This chapter has also covered the performance test and its analysis. Chapter 6 covers a detailed analysis discussion of the authentication and performance testing while addressing number of authentication attacks. The chapter is concluded with a detail comparative analysis of this study with the existing TMIS studies to provide a concise decision based on the findings of the contributions of this study. In Chapter 7, the thesis is concluded while highlighting the individual and overall contributions and discussing the possible future research directions.

REFERENCES

Afsarmanesh, H., Guevara-Masis, V. and Hertzberger, L. O. (2004). Federated management of information for TeleCARE. *Telecare*, 49-62.

Al-Hasan, M., Deb, K. and Rahman, M. O. (2013). User-authentication approach for data security between smartphone and cloud. *Strategic Technology (IFOST), 2013 8th International Forum on*, June 28 2013-July 1 2013. 2-6.

Al-Qahtani, A. A. (2003). *Formal approaches for specifying, enforcing, and verifying security policies*. Doctoral Dissertation. University of Idaho US

Alghamdi, A., Nasir, M., Ahmad, I. and Nafjan, K. A. (2010). An interoperability study of ESB for C4I systems. *Information Technology (ITSim), 2010 International Symposium in*, 15-17 June 2010. 733-738.

Armstrong, N., Nugent, C., Moore, G. and Finlay, D. D. (2013). *Smartphone Application Design and Knowledge Management for People with Dementia*. In Bali, R., Troshani, I., Goldberg, S. and Wickramasinghe, N. (Ed.) *Pervasive Health Knowledge Management*. (135-153). Springer New York.

Asanin, S., Rosengren, P. and Brodén, T. (2013). *Evaluating Energy Profiles as Resource of Context and as Added Value in Integrated and Pervasive Socio-Medical Technologies using LinkSmart Middleware*. In (Ed.) *Wireless Mobile Communication and Healthcare*. (429-436). Springer.

Awasthi, A. and Srivastava, K. (2013). A Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce. *Journal of Medical Systems* 37(5), 1-4.

Bin Muhaya, F. T. (2014). Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system. *Security and Communication Networks*, 101-113.

Bisong, B., Asonganyi, E., Gontarenko, A., Semenov, A. and Veijalainen, J. (2013). *A Mobile Healthcare System for Sub-saharan Africa*. In Godara, B. and Nikita, K. (Ed.) *Wireless Mobile Communication and Healthcare*. (69-78). Springer Berlin Heidelberg.

Bona, J. K. (2013). *WO2012174092 A3*. United States: USPTO.

Boyd, C. and Mathuria, A. (2003). *Password-Based Protocols*. In (Ed.) *Protocols for Authentication and Key Establishment*. (247-288). Springer Berlin Heidelberg.

Brownsell, S., Blackburn, S. and Hawley, M. S. (2008). An evaluation of second and third generation telecare services in older people's housing. *Journal of Telemedicine and Telecare* 14(1), 8-12.

Burrows, M., Abadi, M. and Needham, R. M. (1989). A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 426(1871), 233-271.

Cao, T. and Zhai, J. (2013). Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems* 37(2), 1-7.

Cawley, C. (2013, 18.01.2013). "4 Smartphone Security Risks To Be Aware Of." Retrieved 23.02.2014, 2013, from http://www.makeuseof.com/tag/4-smartphone-security-risks-to-be-aware-of/.

Chen, H.-C. and Prater, E. (2013). Information System Costs of Utilizing Electronic Product Codes in Achieving Global Data Synchronization within the Pharmaceutical Supply Chain Network. *International Journal of Information Systems and Supply Chain Management (IJISSCM)* 6(1), 62-76.

Chen, H.-M., Lo, J.-W. and Yeh, C.-K. (2012). An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems* 36(6), 3907-3915.

Consortium, W. C. (2001). "Web Services Description Language (WSDL) 1.1." from http://www.w3.org/TR/wsdl.

Constantinescu, L., Jinman, K. and Feng, D. D. (2012). SparkMed: A Framework for Dynamic Integration of Multimedia Medical Data Into Distributed m-Health Systems. *IEEE Transactions on Information Technology in Biomedicine,* 16(1), 40-52.

Coskun, B. and Herley, C. (2008). Can "Something You Know" Be Saved?. *Information Security*. Springer Berlin, Heidelberg. 421-440.

Cremers, C. and Mauw, S. *Operational semantics and verification of security protocols*. Springer Science and Business Media, 2012

Cremers, C. J. (2008). The Scyther Tool: Verification, falsification, and analysis of security protocols. *Computer Aided Verification*, 414-418.

Cremers, C. J. F. *Scyther: Semantics and verification of security protocols*. 68(02). Eindhoven University of Technology, 2006.

Dabiri, F., Massey, T., Noshadi, H., Hagopian, H., Lin, C. K., Tan, R., Schmidt, J. and Sarrafzadeh, M. (2009). A Telehealth Architecture for Networked Embedded Systems: A Case Study in In-Vivo Health Monitoring. *IEEE Transactions on Information Technology in Biomedicine,* 13(3), 351-359.

Das, A. and Goswami, A. (2014). An Enhanced Biometric Authentication Scheme for Telecare Medicine Information Systems with Nonce Using Chaotic Hash Function. *Journal of Medical Systems* 38(6), 1-19.

Debiao, H., Jianhua, C. and Rui, Z. (2012). A More Secure Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems* 36(3), 1989-1995.

Demirkan, H. (2013). A Smart Healthcare Systems Framework. *IT Professional* 15(5), 38-45.

Dilmaghani, R., Ghavami, M. and Bobarshad, H. A new paradigm for telehealth implementation. *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, August 31 - September 4. 2010. 3915-3918.

Dilmaghani, R. S., Bobarshad, H., Ghavami, M., Choobkar, S. and Wolfe, C. (2011). Wireless Sensor Networks for Monitoring Physiological Signals of Multiple Patients. *IEEE Transactions on Biomedical Circuits and Systems,* 5(4), 347-356.

Dinh, H. T., Lee, C., Niyato, D. and Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing* 13(18), 1587-1611.

Doukas, C., Pliakas, T. and Maglogiannis, I. (2010). Mobile healthcare information management utilizing Cloud Computing and Android OS. *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, Aug. 31 2010-Sept. 4 2010. 1037-1040.

Eargle, C. B. (2012). The .Net Developer's Guide, Memory and Performance Profiling. 1(1), 02-38. *Telerik*

Eldefrawy, M. H., Alghathbar, K. and Khan, M. K. (2011). OTP-based two-factor authentication using mobile phones. *Information Technology: New Generations (ITNG), 2011 Eighth International Conference*, 327-331.

Elmuti, D. and Topaloglu, O. (2013). ERP systems to the rescue. *Industrial Management* 55(6).

EnNasry, B. and ElKettani, M. D. E.-C. (2011). *Towards an Open Framework for Mobile Digital Identity Management through Strong Authentication Methods*. In (Ed.) *Secure and Trust Computing, Data Management, and Applications*. (56-63). Springer.

Fan, X. and Gong, G. (2013). Securing NFC with Elliptic Curve Cryptography–Challenges and Solutions. *Radio Frequency Identification System Security: RFIDsec'13 Asia Workshop Proceedings*, 97.

FFIEC (2006). *FFIEC*.

Fierrez, J., Galbally, J., Ortega-Garcia, J., Freire, M. R., Alonso-Fernandez, F., Ramos, D., Toledano, D. T., Gonzalez-Rodriguez, J., Siguenza, J. A., Garrido-Salas, J., Anguiano, E., Gonzalez-de-Rivera, G., Ribalda, R., Faundez-Zanuy, M., Ortega, J. A., Cardeñoso-Payo, V., Viloria, A., Vivaracho, C. E., Moro, Q. I., Igarza, J. J., Sanchez, J., Hernaez, I., Orrite-Uruñuela, C., Martinez-Contreras, F. and Gracia-Roche, J. J. (2010). BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications* 13(2), 235-246.

Forum, U. (2000). "The Universal Plug and Play Architecture." from http://upnp.org/resources/upnpresources.zip.

Foster, K. R. (2010). Telehealth in Sub-Saharan Africa: Lessons for Humanitarian Engineering. *IEEE Technology and Society Magazine,* 29(1), 42-49.

Ghani, M. K. A., Bali, R. K., Naguib, R. N. and Marshall, I. M. (2013). *The Analysis and Design of a Pervasive Health Record: Perspectives From Malaysia*. In (Ed.) *Pervasive Health Knowledge Management*. (81-101). Springer.

Gkatzikis, L. and Koutsopoulos, I. (2013). Migrate or not? exploiting dynamic task migration in mobile cloud computing systems. *IEEE Wireless Communications,* 20(3), 24-32.

Goudar, V. A. (2014). *Data-Semantics Driven Power Optimization of Wireless Medical Monitoring Devices,* Doctoral Dissertation. University of California, Log Angeles.

Grzonkowski, S. and Corcoran, P. M. (2011). Sharing cloud services: user authentication for social enhancement of home networking. *IEEE Transactions on Consumer Electronics*, 57(3), 1424-1432.

Gschwind, T., Eshghi, K., Garg, P. K. and Wurster, K. (2002). Webmon: A performance profiler for web transactions. *Advanced Issues of E-Commerce and Web-Based Information Systems, 2002.(WECWIS 2002). Proceedings. Fourth IEEE International Workshop*, 171-176.

Guevara-Masis, V., Afsarmanesh, H. and Hertzberger, L. (2004). *Service-Oriented Architecture of TeleCARE*. In Meersman, R., Tari, Z. and Corsaro, A. (Ed.) *On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops*. (14-16). Springer Berlin Heidelberg.

Günther, M. and Borchert, B. (2013). *Online Banking with NFC-Enabled Bank Card and NFC-Enabled Smartphone*. In Cavallaro, L. and Gollmann, D. (Ed.) *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems*. (66-81). Springer Berlin Heidelberg.

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., Feldman, A. J., Appelbaum, J. and Felten, E. W. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM* 52(5), 91-98.

Hao, X., Wang, J., Yang, Q., Yan, X. and Li, P. (2013). A Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems* 37(2), 1-7.

He, D. and Wang, D. (2014). Robust Biometrics-Based Authentication Scheme for Multiserver Environment. *IEEE Systems Journal*, (99), 1-8.

He, D., Wang, D. and Wu, S. (2013). Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. *Information Technology And Control* 42(2), 105-112.

Honggang, W., Shaoen, W., Min, C. and Wei, W. (2014). Security protection between users and the mobile media cloud. *IEEE Communications Magazine*, 52(3), 73-79.

Hu, J.-Y., Sueng, C.-C., Liao, W.-H. and Ho, C. C. (2012). Android-based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking. *Computing, Communications and Applications Conference (ComComAp), 2012*, 111-116.

Jiang, Q., Ma, J., Lu, X. and Tian, Y. (2014). Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems. *Journal of Medical Systems* 38(2), 1-8.

Jiang, Q., Ma, J., Ma, Z. and Li, G. (2013). A Privacy Enhanced Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems* 37(1), 1-8.

Jucheng, Y., Naixue, X., Vasilakos, A. V., Zhijun, F., Dongsun, P., Xianghua, X., Sook, Y., Shanjuan, X. and Yong, Y. (2011). A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications. *IEEE Systems Journal*, 5(4), 574-583.

Jung, I. Y., Jang, G.-J. and Kang, S.-J. (2014). Secure eHealth-care Service on Self-organizing Software platform. *Smart Computing Review* 4(1), 9-18.

Kao, H.-Y., Cheng, Y.-T. and Chien, Y.-K. (2014). *Develop and Evaluate the Mobile-Based Self-Management Application for Tele-Healthcare Service*. In Ali, M., Pan, J.-S., Chen, S.-M. and Horng, M.-F. (Ed.) *Modern Advances in Applied Intelligence*. (460-469). Springer International Publishing.

Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. *IEEE Security and Privacy,* 7(4), 61-64.

Khan, A., Mat Kiah, M. L., Madani, S., Khan, A. and Ali, M. (2013). Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. *The Journal of Supercomputing,* 66(3), 1687-1706.

Khan, K. M. and Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *IT Professional,* 12(5), 20-27.

Khan, M. K. and Kumari, S. (2013). An Improved User Authentication Protocol for Healthcare Services via Wireless Medical Sensor Networks.

Khan, M. K. and Kumari, S. (2014). Cryptanalysis and Improvement of "An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems". *Security and Communication Networks* 7(2), 399-408.

Kim, M. (2006). *Cryptanalysis and enhancement of authentication protocols*.

Kumari, S., Khan, M. and Kumar, R. (2013). Cryptanalysis and Improvement of 'A Privacy Enhanced Scheme for Telecare Medical Information Systems'. *Journal of Medical Systems,* 37(4), 1-11.

Kumari, S. and Khan, M. K. (2013a). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. *International Journal of Communication Systems*, 88-101.

Kumari, S. and Khan, M. K. (2013b). More secure smart card-based remote user password authentication scheme with user anonymity. *Security and Communication Networks,* 134-148.

Kusters, R. and Truderung, T. (2009). Using ProVerif to analyze protocols with Diffie-Hellman exponentiation. *22nd IEEE Computer Security Foundations Symposium, 2009. CSF'09*, 157-171.

Kwak, Y. H., Park, J., Chung, B. Y. and Ghosh, S. (2012). Understanding End-Users Acceptance of Enterprise Resource Planning (ERP) System in Project-Based Sectors. *IEEE Transactions on Engineering Management* 59(2), 266-277.

Ladyzynski, P., Wojcicki, J. M. and Foltynski, P. (2012). *Effectiveness of the Telecare Systems*. In Jobbágy, Á. (Ed.) *5th European Conference of the*

International Federation for Medical and Biological Engineering. (937-940). Springer Berlin Heidelberg.

Lakshmiraghavan, B. (2013). *Two-Factor Authentication*. In (Ed.) *Pro ASP.NET Web API Security*. (319-343). Apress.

Lamprinakos, G., Asanin, S., Rosengren, P., Kaklamani, D. and Venieris, I. (2012). *Using SOA for a Combined Telecare and Telehealth Platform for Monitoring of Elderly People*. In Nikita, K., Lin, J., Fotiadis, D. and Arredondo Waldmeyer, M.-T. (Ed.) *Wireless Mobile Communication and Healthcare*. (233-239). Springer Berlin Heidelberg.

Lee, H.-C. and Chang, S.-H. (2012). RBAC-Matrix-Based EMR Right Management System to Improve HIPAA Compliance. *Journal of Medical Systems* 36(5), 2981-2992.

Lee, S.-W., Kim, H.-S. and Yoo, K.-Y. (2005). Efficient verifier-based key agreement protocol for three parties without server's public key. *Applied Mathematics and Computation* 167(2), 996-1003.

Lee, T.-F. (2013). An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems. *Journal of Medical Systems*, 37(6), 1-9.

Lee, T.-F. and Liu, C.-M. (2013). A Secure Smart-Card Based Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems* 37(3), 1-8.

Leicher, A., Schmidt, A. and Shah, Y. (2012). *Smart OpenID: A Smart Card Based OpenID Protocol*. In Gritzalis, D., Furnell, S. and Theoharidou, M. (Ed.) *Information Security and Privacy Research*. (75-86). Springer Berlin Heidelberg.

Li, S.-H., Wang, C.-Y., Lu, W.-H., Lin, Y.-Y. and Yen, D. (2012). Design and Implementation of a Telecare Information Platform. *Journal of Medical Systems*, 36(3), 1629-1650.

Liang, Z. (2008). *On formal methods of checking cryptographic protocols*. 3346791 Ph.D., Doctoral Dissertation. University of Houston.

Lin, H.-Y. (2013). On the Security of A Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*, 37(2), 1-5.

Lin, T.-H. and Lee, T.-F. (2014). Secure Verifier-Based Three-Party Authentication Schemes without Server Public Keys for Data Exchange in Telecare Medicine Information Systems. *Journal of Medical Systems*, 38(5), 1-9.

Maarop, N. and Win, K. (2012). Understanding the Need of Health Care Providers for Teleconsultation and Technological Attributes in Relation to The Acceptance of Teleconsultation in Malaysia: A Mixed Methods Study. *Journal of Medical Systems*, 36(5), 2881-2892.

Medvedev, O., Kobelev, A., Schookin, S., Jatskovsky, M., Markarian, G. and Sergeev, I. (2007). *Smartphone-based Approach for Monitoring Vital Physiological Parameters in Humans*. In Magjarevic, R. and Nagel, J. H. (Ed.) *World Congress on Medical Physics and Biomedical Engineering 2006*. (4020-4022). Springer Berlin Heidelberg.

Megat Ali, M., Jahidin, A. H., Nasir, N. F. M., Saidatul, A., Zakaria, Z., Salleh, A. F. and Mustafa, N. (2008). *Malaysia and Telecare — A Preliminary Study*. In Abu Osman, N., Ibrahim, F., Wan Abas, W., Abdul Rahman, H. and Ting, H.-N. (Ed.) *4th Kuala Lumpur International Conference on Biomedical Engineering 2008*. (862-866). Springer Berlin Heidelberg.

Merkle, R. C. (1990). One way hash functions and DES. *Advances in Cryptology—CRYPTO'89 Proceedings*, 428-446.

Mishra, D. (2013). A Study On ID-based Authentication Schemes for Telecare Medical Information System. *arXiv preprint arXiv:1311.0151*.

Mishra, D., Mukhopadhyay, S., Chaturvedi, A., Kumari, S. and Khan, M. (2014a). Cryptanalysis and Improvement of Yan et al.'s Biometric-Based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*, 38(6), 1-12.

Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M. and Chaturvedi, A. (2014b). Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce. *Journal of Medical Systems*, 38(5), 1-11.

Monteagudo, J. L., Salvador, C. H. and Kun, L. (2014). Envisioning patient safety in Telehealth: a research perspective. *Health and Technology*, 1-15.

Mosa, A., Yoo, I. and Sheets, L. (2012). A Systematic Review of Healthcare Applications for Smartphones. *BMC Medical Informatics and Decision Making* 12(1), 1-31.

Motoyama, T. and Tsay, D. (1996).

Munkelt, T. and Völker, S. (2013). ERP systems: aspects of selection, implementation and sustainable operations. *International Journal of Information Systems and Project Management,* 1(2), 25-39.

Mylonas, A., Dritsas, S., Tsoumas, B. and Gritzalis, D. (2012). *On the feasibility of malware attacks in smartphone platforms*. In (Ed.) *E-Business and Telecommunications*. (217-232). Springer.

Omri, F., Foufou, S., Hamila, R. and Jarraya, M. (2013). Cloud-based mobile system for biometrics authentication. *ITS Telecommunications (ITST), 2013 13th International Conference on*, 5-7 Nov. 2013. 325-330.

PCI-DSS (2008). *8.3*. PCI Security Standard Council: PCI

Pinciroli, F., Corso, M., Fuggetta, A., Masseroli, M., Bonacina, S. and Marceglia, S. (2011). Telemedicine and E-Health. *IEEE Pulse,* 2(3), 62-70.

Qiang, D., Yuhong, Y. and Vasilakos, A. V. (2012). A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing. *IEEE Transactions on Network and Service Management*, 9(4), 373-392.

Rashid, U., Schmidtke, H. and Woo, W. (2007). *Managing Disclosure of Personal Health Information in Smart Home Healthcare*. In Stephanidis, C. (Ed.) *Universal Access in Human-Computer Interaction. Ambient Interaction*. (188-197). Springer Berlin Heidelberg.

Rashvand, H. F., Salah, K., Calero, J. M. A. and Harn, L. (2010). Distributed security for multi-agent systems–review and applications. *IET information security,* 4(4), 188-201.

Rassan, I. A. L. and AlShaher, H. (2014). Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA). *International Conference on Computational Science and Computational Intelligence (CSCI), 2014*, 10-13 March 2014. 157-161.

Salmela, P. and Melén, J. (2007). *Host Identity Protocol Proxy*. In Filipe, J., Coelhas, H. and Saramago, M. (Ed.) *E-business and Telecommunication Networks*. (126-138). Springer Berlin Heidelberg.

Sediyono, E., Santoso, K. I. and Suhartono (2013). Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS. *International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013*, 22-25 Aug. 2013. 1604-1608.

Sendra, S., Granell, E., Lloret, J. and Rodrigues, J. P. C. (2013). Smart Collaborative Mobile System for Taking Care of Disabled and Elderly People. *Mobile Networks and Applications*, 1-16.

Shashidhar, N. (2013). *WO2013019701 A1*. United States: US Patent Office.

Siddiqui, Z., Abdullah, A., Khan, M. and Alghamdi, A. (2013). Smart Environment as a Service: Three Factor Cloud Based User Authentication for Telecare Medical Information System. *Journal of Medical Systems*, 38(1), 1-14.

Siddiqui, Z., Abdullah, A. H., Khan, M. K. and Alghathbar, K. (2011). Analysis of enterprise service buses based on information security, interoperability and high-availability using Analytical Hierarchy Process (AHP) method. *Journal of Physical Sciences*, 6(1), 35-42.

Sintonen, S. and Immonen, M. (2013). Telecare services for aging people: Assessment of critical factors influencing the adoption intention. *Computers in Human Behavior* 29(4), 1307-1317.

Smyth, B. (2011). *Formal verification of cryptographic protocols with automated reasoning*, University of Birmingham.

Stowe, S. and Harding, S. (2010). Telecare, telehealth and telemedicine. *European Geriatric Medicine* 1(3), 193-197.

Sulaiman, R., Sharma, D., Ma, W. and Tran, D. (2007). *A Multi-agent Security Framework for e-Health Services*. In Apolloni, B., Howlett, R. and Jain, L. (Ed.) *Knowledge-Based Intelligent Information and Engineering Systems*. (547-554). Springer Berlin Heidelberg.

Sundar, S. S., Bellur, S. and Jia, H. (2012). *Motivational Technologies: A Theoretical Framework for Designing Preventive Health Applications*. In Bang, M. and Ragnemalm, E. (Ed.) *Persuasive Technology. Design for Health and Safety*. (112-122). Springer Berlin Heidelberg.

Supriyanto, E. (2011). A suitable telehealth model for developing countries. *Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2011 2nd International Conference*, 8-9 Nov. 2011. 414-414.

Syverson, P. and Cervesato, I. (2001). *The Logic of Authentication Protocols*. In Focardi, R. and Gorrieri, R. (Ed.) *Foundations of Security Analysis and Design*. (63-137). Springer Berlin Heidelberg.

Tan, Z. (2014). A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 38(3), 1-9.

TeleCare, G. S. (1987). "Telecare History." from http://www.telecarehomemonitoring.com/about-telecare/history/.

Tien-Ho, C., Hsiu-lien, Y. and Wei-Kuan, S. (2011). An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing. *Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference*, 28-30 June 2011. 155-159.

Urien, P. and Piramuthu, S. (2014). *Securing NFC Mobile Services with Cloud of Secure Elements (CoSE)*. In Memmi, G. and Blanke, U. (Ed.) *Mobile Computing, Applications, and Services*. (322-331). Springer International Publishing.

Vassis, D., Zafeiris, B., Skourlas, C. and Belsis, P. (2012). An Ad Hoc-Based ERP for Medical Treatment Provision in Crisis Conditions. *Informatics (PCI), 2012 16th Panhellenic Conference*, 5-7 Oct. 2012. 439-444.

Wei, J., Hu, X. and Liu, W. (2012). An Improved Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 36(6), 3597-3604.

Wen, F. (2013). A Robust Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care. *Journal of Medical Systems,* 37(6), 1-9.

Wortmann, J. C., Boonstra, A., Broekhuis, M., van Meurs, J., van Offenbeek, M., Westerman, W. and Wijngaard, J. (2009). Is Telecare Feasible? Lessons from an In-depth Case Study. *Enabling Technologies: Infrastructures for Collaborative Enterprises, 2009. WETICE '09. 18th IEEE International Workshops*, June 29 2009-July 1 2009. 246-251.

Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C. and Chung, Y. (2012). A Secure Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 36(3), 1529-1535.

Xiaoliang, W., Qiong, G., Bingwei, L., Zhanpeng, J. and Yu, C. (2014). Enabling Smart Personalized Healthcare: A Hybrid Mobile-Cloud Approach for ECG Telemonitoring. *IEEE Journal of Biomedical and Health Informatics,* 18(3), 739-745.

Xie, Q., Zhang, J. and Dong, N. (2013). Robust Anonymous Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems,* 37(2), 1-8.

Yan, S. Y. (2012). *Computational Number Theory and Modern Cryptography*: John Wiley and Sons.

Yan, X., Li, W., Li, P., Wang, J., Hao, X. and Gong, P. (2013). A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 37(5), 1-6.

Yau, W.-C. and Phan, R. W. (2013). Security Analysis of a Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 37(6), 1-9.

Yoon, E.-J., Lee, W.-S. and Yoo, K.-Y. (2007). *Secure PAP-Based RADIUS Protocol in Wireless Networks*. In Huang, D.-S., Heutte, L. and Loog, M. (Ed.) *Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques*. (689-694). Springer Berlin Heidelberg.

Zarandioon, S. (2012). *Improving the security and usability of cloud services with user-centric security models*, Rutgers, The State University of New Jersey.

Zhang, Z. and Qi, Q. (2014). An Efficient RFID Authentication Protocol to Enhance Patient Medication Safety Using Elliptic Curve Cryptography. *Journal of Medical Systems,* 38(5), 1-7.

Zhu, Z. (2012). An Efficient Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 36(6), 3833-3838.

Zibin, Z., Zhou, T. C., Lyu, M. R. and King, I. (2012). Component Ranking for Fault-Tolerant Cloud Applications. *IEEE Transactions on Services Computing*, 5(4), 540-550.

Ziyad, S. and Kannammal, A. (2014). *A Multifactor Biometric Authentication for the Cloud*. In Krishnan, G. S. S., Anitha, R., Lekshmi, R. S.et al (Ed.) *Computational Intelligence, Cyber Security and Computational Models*. (395-403). Springer India.