Towards Designing an Efficient Authentication Scheme for RFID-based Healthcare Applications in Vehicular Mobile Cloud

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Engineering

in

Information Security

Submitted By

Kuljeet Kaur
(Roll No. : 801333010)

Under the Supervision of:

Dr. Neeraj Kumar
Associate Professor
CSED

Ms. Maggi Bansal
Lecturer
CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2015

Certificate

I hereby certify that the work which is being presented in the thesis entitled, *"Towards Designing an Efficient Authentication Scheme for RFID-based Healthcare Applications in Vehicular Mobile Cloud"*, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Neeraj Kumar* and *Ms. Maggi Bansal*.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:
(Kuljeet Kaur)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Neeraj Kumar)
Associate Professor
CSED
Thapar University
Patiala

(Ms. Maggi Bansal)
Lecturer
CSED
Thapar University
Patiala

Countersigned by:

(Dr. Deepak Garg)
Head
CSED
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean
Academic Affairs
Thapar University
Patiala

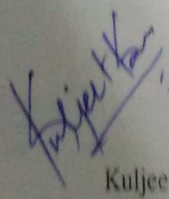
Acknowledgment

I have been waiting long for this moment to acknowledge all those who contributed in building this work. It is my pleasure to thank all of them here. First of all, I offer my sincere gratitude to my supervisors, *Dr. Neeraj Kumar* and *Ms. Maggi Bansal*, for accepting to be my supervisors. Without their help and encouraging advice, this work would have never begun. I am deeply indebted to them for providing me wonderful research atmosphere and platform to explore my research to the fullest.

I would also extend my gratitude to *Dr. Maninder Singh* who played a significant role in my clarifying my doubts related to security fundamentals. I am also grateful to *Dr. Deepak Garg*, Head, CSED for providing me the opportunity to conduct my research work. I would also like to thank the Director of the institute, *Prof. Prakash Gopalan* for his continuous support.

My special thanks goes to my friends for discussing thoughts and sharing all ups and downs with me during the course of this work. At the same time I would also like to thank all my colleagues for their continuous support.

Last but not the least I would like to thank my parents and family members, who made me capable of reaching this point of life and for giving me their kind support and love. I dedicate my work to them.



Kuljeet Kaur
ME (Information Security)
Roll No.:801333010

Copyright Form

SPRINGER LICENSE
TERMS AND CONDITIONS

Jun 19, 2015

This is a License Agreement between Kuljeet Kaur ("You") and Springer ("Springer") provided by Copyright Clearance Center ("CCC"). The license consists of your order details, the terms and conditions provided by Springer, and the payment terms and conditions.

All payments must be made in full to CCC. For payment instructions, please see information listed at the bottom of this form.

License Number	3652470198486
License date	Jun 19, 2015
Licensed content publisher	Springer
Licensed content publication	Peer-to-Peer Networking and Applications
Licensed content title	An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud
Licensed content author	Neeraj Kumar
Licensed content date	Jan 1, 2015
Type of Use	Thesis/Dissertation
Portion	Full text
Number of copies	1
Author of this Springer article	Yes and you are a contributor of the new work
Order reference number	8727825555
Title of your thesis / dissertation	TOWARDS DESIGNING AN EFFICIENT AUTHENTICATION SCHEME FOR RFID BASED HEALTHCARE APPLICATIONS IN VEHICULAR MOBILE CLOUD
Expected completion date	Aug 2015
Estimated size(pages)	50
Total	0.00 CAD
Terms and Conditions	

Introduction
The publisher for this copyrighted material is Springer Science + Business Media. By clicking "accept" in connection with completing this licensing transaction, you agree that the following terms and conditions apply to this transaction (along with the Billing and Payment terms and conditions established by Copyright Clearance Center, Inc. ("CCC"), at the time that you opened your Rightslink account and that are available at any time at http://myaccount.copyright.com).

Limited License
With reference to your request to reprint in your thesis material on which Springer Science and Business Media control the copyright, permission is granted, free of charge, for the use indicated in your enquiry.

Abstract

Radio Frequency Identification (RFID) is one of the leading wireless technologies in the field of Automatic Identification and Data Capture (AIDC). With its increasing popularity amongst the researchers and industries, it has been successful in paving its way to the healthcare domain. Potential healthcare applications of RFID are limited to tracking of assets and monitoring of patients inside the hospital premises. However, with an exponential increase in internet users, there is a steep increase in mobile healthcare solutions. So, this thesis proposes a novel healthcare application using RFID-enabled devices, which aims to monitor the patients' health while they travel outside the hospital premises. Integration of vehicular cloud computing (VCC) and intelligent transportation systems (ITS) has been proposed in this work to provide uninterrupted services to the patients even on-the-fly. However, potential security breaches in such an environment may lead to various types of issues such as-information leakage, identity revelation, tracking, etc. Thus, privacy needs to be embedded in such applications so as to maintain highest levels of privacy and authenticity at all times.

In order to address these issues, this thesis proposes an intelligent authentication scheme for RFID-enabled healthcare applications in VCC environment. In the proposed scheme, both server and tag authentications are protected by the strong Elliptical Curve Cryptography (ECC) based key generation mechanism. The proposed scheme is found to be secure as it establishes mutual authentication between the server and tags while protecting against replay, tracking, eavesdropping, cloning, and forward secrecy risks. Moreover, evaluation of the proposed authentication scheme with respect to various parameters such as-storage requirements, communicational overhead generated, and computational complexity provides better performance in comparison with the existing schemes. In addition to this, the formal security verification of the proposed protocol is also presented using an automated tool-AVISPA. The obtained results indicate that the protocol is suitable for RFID-enabled devices and provides better security than its previous counterparts.

Keywords: Authentication Mechanism, Elliptic curve cryptography, Healthcare Applications, Radio frequency identification, and Petri Net.

Contents

List of Figures

List of Tables

List of Symbols

a, b	Coefficients of the elliptic curve under reference.
AS	Central authentication server.
E	Elliptic curve under reference.
$G(p)$	Finite prime field.
$G(2^m)$	Finite polynomial binary field.
$h(.)$	One-way hash function.
n	Order of G(P).
p	Large prime number.
P	Generator point for the elliptic curve.
P_{CA}	Place related to authentication server's request which successfully completes the authentication process.
P_{FA}	Place related authentication server's request in failed state.
P_{FR}	Place related to RFID tag's request in failed state.
P_{Ii}	Place related to illegitimate RFID tag's request.
P_{Li}	Place related to legitimate RFID tag's request.
P_{LI}, P_{II}	Place related to RFID tag's request in idle state.
P_{LM}, P_{IM}	Place related to RFID tag's request generating authentication messages.
P_{LQ}, P_{IQ}	Place related to RFID tag's request in waiting state and waiting to be serviced.
P_{LS}, P_{IS}	Place related to RFID tag's request in service state.
P_{NP}	Place related to RFID tag's request which proceeds to next phase of authentication.
P_{Ri}	Place related to real authentication server's request.
P_{RI}, P_{SI}	Place related to authentication server's request at idle state.
P_{RM}, P_{SM}	Place related to authentication server's request generating messages.
P_{RQ}, P_{SQ}	Place related to authentication server's request in waiting state and waiting to be serviced.
P_{RS}, P_{SS}	Place related to authentication server's request in service state.
P_{Si}	Place related to spoofed authentication server's request.
RT	RFID Tag involved in authentication process.
T_{Ii}	Transaction related to illegitimate RFID tag's request.

T_{Li}	Transaction related to legitimate RFID tag's request.
T_{Ri}	Transaction related to real authentication server's request.
T_{Si}	Transaction related to spoofed authentication server's request.
x_S	Private key of server.
X_S	Public key of server.
x_T	Private key of tag.
X_T	Public key of tag.
$\|\|$	Concatenation operation.
$\lambda_{LT}, \lambda_{IT}$	Message generating rate of legitimate and illegitimate tags respectively.
$\lambda_{RS}, \lambda_{SS}$	Message generating rate of real and spoofed server respectively.
μ_A	Service rate of authentication server.
μ_R	Service rate of RFID tag.
γ_A	Failure rate of tag's request.
γ_{RT}	Failure rate of server's request.
$(1)\ldots$	Signifies that successful tag identification during phase-2 leads to phase-3.

List of Abbreviations

AVISPA	Automated Validation of Internet Security Protocols and Validation.
ECC	Elliptic Curve Cryptography.
ECDLP	Elliptic Curve Discrete Logarithm Problem.
ITS	Intelligent Transportation System.
LF	Low Frequency.
PN	Petri-net.
RFID	Radio Frequency Identification.
RSU	Road side unit.
UHF	Ultra High Frequency.
VANETS	Vehicular Ad Hoc Networks.
VCC	Vehicular Cloud Computing.
V2I	Vehicle-to-infrastructure.
V2V	Vehicle-to-vehicle.
WBAN	Wireless Body Area Network.

Chapter 1

INTRODUCTION

Radio Frequency Identification (RFID) is one of the most popular technologies in the field of automatic identification of objects ranging from assets and equipments to living beings. The seeds of this novel technology were laid during the World War-II (1939 to 1945). During that time, it was simply used against target detection and to differentiate between friend and foe weapons. This technology has gained huge momentum during the last couple of years. Today, numerous applications such as-automatic asset tracking, logistics, tracking and locating medical equipments, laboratory samples, garbage, humans and many more are supported by RFID [1–3]. The list is endless with RFID leaving its marks in almost each and every field ranging from healthcare systems to supply management systems and passport and baggage identification systems at airports [1].

RFID's dropping cost and distinct features have played a vital role in accelerating its wide scale adoption. Some of these features are mentioned as follows. Firstly, the devices equipped with RFID tags can be uniquely identified using radio waves. Secondly, it supports passive and battery free communication model between the RFID tags and readers [4]. The most important feature of RFID is that, it is based on the contactless identification scheme, unlike conventional bar code technology. Due to these reasons, RFID technology has been successful in replacing the conventional bar code technology by a large extent [1, 3]. These differences between the two technologies has changed the face of number of industries where asset, object, human, animal, etc. monitoring and tracking is of utmost importance.

A typical RFID system is depicted in Fig. 1.1. It comprises of three main components: a RFID-enabled reader, one or more tags, and a back-end server. Reader (also called an interrogator) is device that helps to identify the RFID-enabled devices called tags [2, 3]. It identifies the objects with the help of radio waves by emitting a continuous wave. In return to these waves, tags modulate the backscattered signals to respond with the required data.

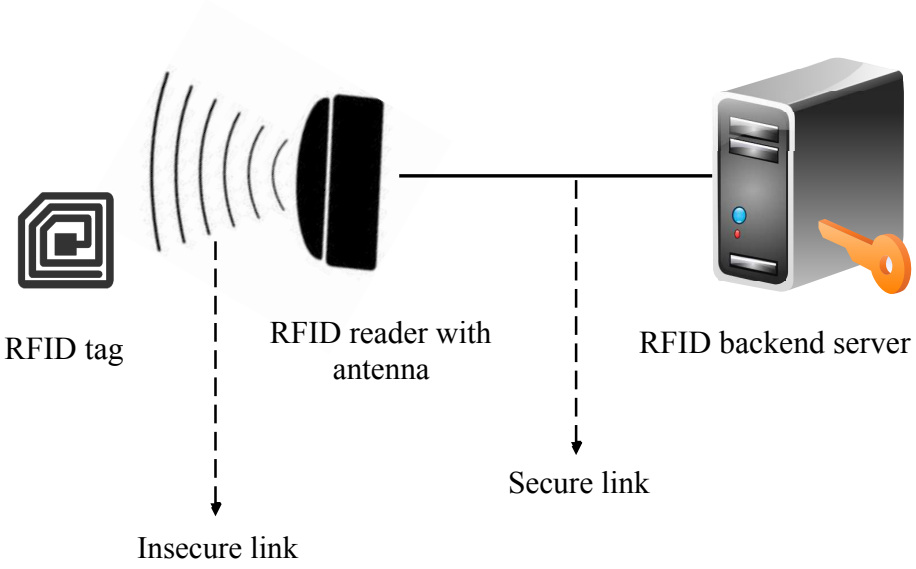


Figure 1.1: A typical RFID system comprising of: A reader, tag, and back-end server.

Finally, the interrogator decodes the received signals to successfully identify the RFID-tagged objects. RFID tags or responders are basically miniature chips that are tied to the objects that needs tracking and remote identification. These tags can be broadly classified into three categories as-active, passive and semi-passive [2,5,6]. On the other hand, RFID-enabled server is a central repository of tag-reader related data and information. Often, these servers play a crucial role in validating the information shared by tags and maintaining their real-time tracking information.

RFID has benefited the healthcare systems immensely. It is being utilized in the tracking of laboratory samples, monitoring of severely ill patients, tracking of hospital assets, etc [1–3]. Tan *et al.* [1] gave a comprehensive study related to the implementation of RFID-enabled systems in the healthcare industry. The authors have classified the RFID technology applications in 5 prominent domains with respect to healthcare industry as: i) Medical asset tracking, ii) Patient identification, iii) Patient tracking, iv) Anti-counterfeiting, and v) Medication safety. In addition to this, many researchers and several industries are also working of the concept of RFID-implant systems [7,8]. Moreover, the use of RFID for clinical purposes has been declared safe by the US Food and Drug Administration (FDA) [7]. Thus, the use of RFID-based systems has become quite ubiquitous across the healthcare industry and its wide scale adoption across various operations necessitates addressing its related security issues. These issues have been extensively explored amongst the academia and industry. Thus, several authentication protocols have been proposed in the literature in order to enhance the security of RFID-related applications. However, some of these protocols purely target resistance against security attacks, while a few others target the stringent

computational resources of RFID tags. Thus, it is essential to maintain a trade-off between efficiency and security while designing secure authentication protocols for RFID devices.

This thesis deals with the implementation of RFID in the healthcare domain to provide services to the passengers on wheels. This means that RFID-enabled devices would be integrated with existing vehicular ad hoc networks (VANETS) to capture and forward the patients' physiological data to a central server. This would result in generation of enormous amount of data, which would require dedicated resources in terms of its storage, processing and management. Thus, a cloud based approach provides an attractive solution to handle these challenges on a real time basis to save countless lives. So, this thesis proposes a novel architecture that deals with integration of RFID coupled VANETs with the cloud computation platform. This coupling has the potential to unleash greater possibilities in terms of higher scalability, faster processing, immense storage, greater flexibility and reliability. This helps to reduce the response of the medical services available on the fly and provides more accurate and quicker information than ever before. Essentially, this coupling provides attractive options to create a cyber-physical system in which vehicles act as the data collector and cloud as the data provider.

Furthermore, this thesis also proposes an efficient authentication mechanism for enhancing the security of the RFID-based healthcare system. This enables secure communication between authenticated RFID tags and the centralized server via RFID readers. The entire authentication mechanism is based upon the lightweight Elliptic Curve Cryptography (ECC) technique. It is one of the most secure techniques in public key cryptography till date. ECC comes into play where the requirements with respect to security of data, computational resources, and battery life of the underlying device need to be justified in an efficient and scalable manner. Thus, ECC-based authentication mechanism in the proposed healthcare scheme seems to be a viable option keeping in view the security of patients' related data and reduced computational resources of RFID devices.

The rest of the thesis is organized as follows. Chapter 2 highlights the research progress done in the field in RFID and ECC. Chapter 3 presents the need and challenges of implementing the ECC-based authentication scheme for RFID-equipped healthcare applications. It also highlights the main contributions of this work. Detailed description about the proposed healthcare scheme and the related authentication protocol is presented in Chapter 4. Chapter 5 presents the summative overview of the security features offered by the proposed scheme. Chapter 6 provides the performance evaluation of the scheme with respect to existing schemes. The formal analysis of the proposed scheme is elaborated using widely accepted tool-Automated Validation of Internet Security Protocols and Applications (AVISPA). Finally, research directions and conclusions are summarized in Chapter 7.

Chapter 2

LITERATURE SURVEY

This chapter highlights the RFID technology with respect to the various existing proposals. It has been extensively investigated with respect to numerous authentication mechanisms, security and privacy issues, and contention resolution schemes. This chapter highlights some of the prominent works specifically related to authentication protocols in RFID-enabled systems. In addition to this, the chapter also provides preliminary details about ECC and Petri-nets (PNs).

2.1 Related Work

A number of authentication protocols have been proposed in the context of RFID-enabled applications [9–23]. The main challenge in the implementation of these protocols is particularly the limited computational and storage capacity of the RFID-enabled devices. These protocols range from server-less authentication mechanism to purely server-based authentication schemes. Moreover, these authentication protocols also differ with respect the cryptographic techniques used. These techniques range from purely hash-based functions to pseudo random number generator algorithms and robust public key cryptographic approaches. The preferred choice however, in this context, is that of ECC-based protocols due to their inherit capacity of smaller key sizes and better security in comparison with other cryptographic techniques [24]. This segment explores a few of these related protocols and architectures which have been proposed so far.

The cryptographic approaches proposed in the literature so far, can be categorized into two broad categories: i) Non-public key cryptosystem, and ii) public key cryptosystem. The former cryptosystems comprise of various simplistic approaches like one-way hash functions, various bit-wise operations (OR, AND, OR, etc.), pseudo random number generators, CRC, etc. On the other hand, the latter comprises on more complex but more secure

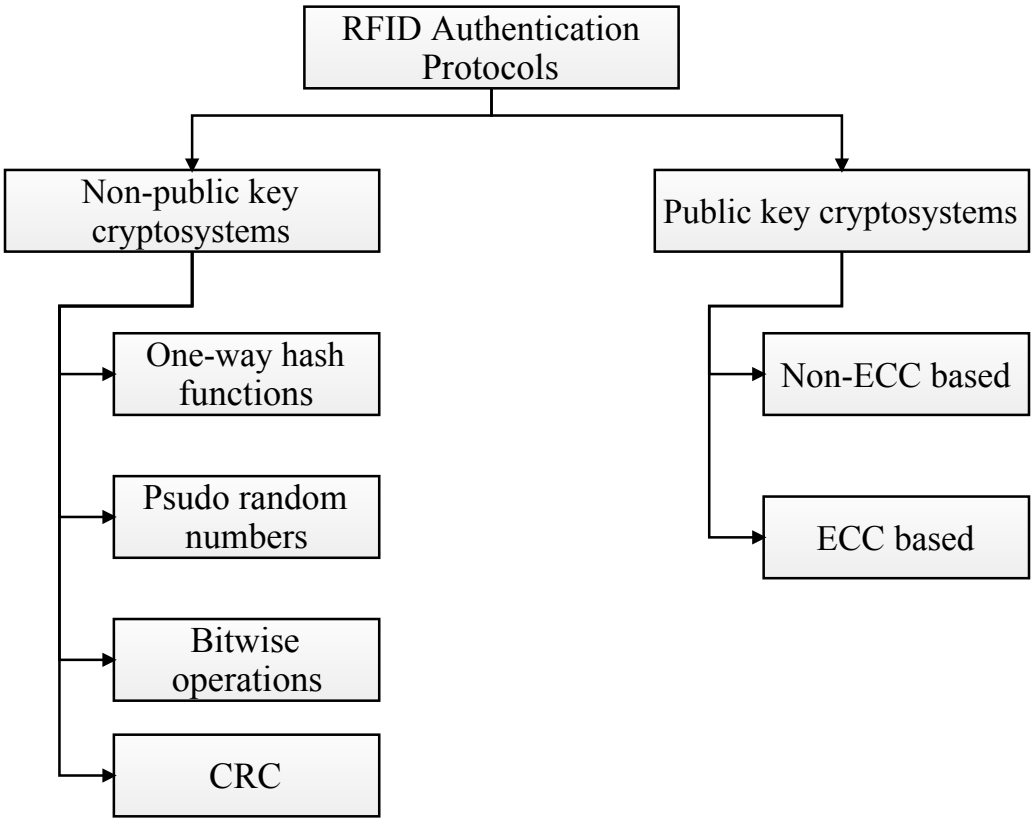


Figure 2.1: Classification of RFID-based authentication schemes.

cryptographic techniques such as-RSA, AES, ECC, etc. The public key cryptographic approaches are further classified into: ECC based and non-ECC based types. Fig. 2.1 depicts this classification of RFID-based authentication schemes.

Among the non-public key cryptosystem based protocols, Le *et al.* [25] proposed an authentication protocol along with an authenticated key exchange mechanism. The authors suggested that their protocol was highly secure and light weight for implementation on RFID devices. It was purely based on pseudo random generation of bits. Furthermore, the authors claimed that their protocol was secure against certain attacks such as-anonymity, forward secrecy, availability, and authenticity. However, Chou *et al.* [22] and Duc *et al.* [26] independently proved that this protocol was prone to de-synchronization and DOS attacks respectively. In another work, Liu and Bailey [27] designed a privacy and authentication protocol (PAP) specifically for supply chain management. The authors suggested that the protocol was capable of providing privacy and authentication in passive RFID-enabled systems. Unfortunately, PAP was found to be susceptible to location tracking and tag spoofing by Chou *et al.* [22].

Yu *et al.* [5] proposed a RFID-based authentication protocol based on the implementa-

tion of hash functions. The authors claimed the security of the said protocol on the basis of an underlying hash function. Unfortunately, Chao *et al.* [14] proved that this protocol was vulnerable to information leakage attack. In another work, Chen *et al.* [15] proposed a low cost authentication protocol particularly for RFID-based systems using hash functions. The authors claimed that the protocol was efficient and was resilient against replay and forward secrecy attacks. However, Chao *et al.* [14] proved that the protocol was susceptible to tag authentication and traceability attacks. Some other protocols which also fall under the non-public key cryptosystem category are described in [28, 29, 29–31].

The above mentioned non-public key cryptographic approaches are suitable for RFID systems in terms of reduced computational and storage cost. However in terms of security, these approaches cannot match the public-key cryptographic schemes, which tend to provide higher security. Thus, this segment explores the research works in this direction. For instance, Won *et al.* [11], proposed an authentication protocol without the need of a central database server which was based on AES-128. The authors suggested that their protocol was suitable for low cost passive RFID devices in comparison with ECC and was resilient against certain security attacks. Unfortunately, this notion of Won *et al.*'s work was proved to be invalid in [12], where Jialiang *et al.* justified that the protocol leads to location tracking. Moreover, the scheme was found to be unsuitable for low cost RFID systems. In [32], Chen *et al.* proposed an authentication protocol based on the concept of quadratic residues and hash function. The authors proposed that their protocol provided protection against a number of security attacks including mutual authentication, anonymity, tracking, replay, etc. However, Cao *et al.* [33] demonstrated that this protocol could not resist impersonation attacks. In addition to this, Yeh *et al.* [34] also found certain loopholes in Chen *et al.*'s work and claimed that the protocol was prone to location privacy and replay attacks.

Ahamad *et al.* [9] proposed an ECC-based RFID authentication protocol (ERAP) to counterfeit the security issues related to tracking, cloning, eavesdropping, and physical attacks. This protocol worked on the notion of off-line back-end server. It also provided the mutual authentication between the two parties, i.e., RFID reader and tags. In another work, Ahamad *et al.* [10] proposed another simple mutual authentication mechanism. The major attraction of this mechanism was that, it was based on sever-less approach, i.e., it did not involve any back-end server for authenticating the two parties. This protocol too defeated various security attacks such as-tracking, cloning, and eavesdropping. In addition to this, Liao *et al.* [16] compared a number of ECC-based protocols proposed for RFID systems from the context of security. Along with this, the authors also proposed an ECC-based authentication mechanism with secure ID-verifier transfer protocol. The authors proposed that their proposed scheme was efficient and resilient against major security attacks includ-

ing eavesdropping, traffic analysis, DOS, and privacy attacks. However, Peeters *et al.* [17] proved that protocol proposed by Liao *et al.* did not satisfy the mutual authentication and was vulnerable to various attacks like tag masquerade, server spoofing, tag cloning, and location tracking.

Druml *et al.* [21] also proposed an ECC-based protocol for the resource constrained devices and applications. The author suggested that the protocol was flexible enough to be implemented in RFID and near field communication (NFC) domains. Furthermore, the scheme was capable of carrying out the authentication between RFID-enabled reader and smart cards. All the extensive ECC-based calculations were performed on RFID readers' end. Moreover, the authors have backed their protocol with appropriate test bed results and depicted that it require 26 ms on an average to process the proposed authentication mechanism. However, Chou [22] independently proposed an authentication protocol for RFID based applications based on ECC. The author proposed this protocol after performing the microanalysis of other protocols and suggested that the proposed protocol was capable enough to overcome the shortcomings of the previously analyzed protocols. He proposed that the protocol was resilient against a number of security attacks like replay, impersonation, tracking and forward secrecy attacks. Unfortunately, Frasah [23] reviewed Chou's work and showed that it was vulnerable to impersonation, location tracking and forward privacy. He further proved that Chou's protocol did not support mutual authentication also.

In another work, Deursen *et al.* [18] and Bringer *et al.* [19] depicted that the protocol proposed by Lee *et al.* [20] was also vulnerable to replay and tracking attacks. Lee *et al.* proposed an ECC-based protocol which was secure against various types of inside attacks in the networks. Godor *et al.* [35] also designed a mutual authentication protocol for low cost RFID systems based on ECC. The authors proposed that the protocol was secure against replay attack, forward secrecy and tracking attacks. However, the protocol was found to be insensitive with respect to forward secrecy and replay attack in [22]. In addition to this, Batina *et al.* [36] also gave an ECC-based protocol for authentication between RFID tags and readers. Unfortunately, the protocol was found to be unsafe for RFID applications in [20]. Moreover, Liao and Hsiao [16] also demonstrated that the protocol suffered from scalability issues and was unsafe against forward secrecy attacks.

Apart from the above mentioned research works which focused primarily on RFID's security, a number of research proposal have been proposed in the literature pertaining to RFID implementation in healthcare industry. The upcoming segment provides a brief review of the existing state-of-art in this direction. For instance, Yu *et al.* [5] proposed an efficient data collection and dissemination RuBee (IEEE 1902.1 Standard) based system in the field of telemedicine. The author proposed that RuBee tags and controllers oper-

ate at lower frequency bands and hence, are more reliable than RFID tags. According to the authors, the RFID tags are not re-programmable and thus, RuBee outperforms them. However, Chen *et al.* [6] proposed an architecture model for e-healthcare system based on 2-generation RFID system that falsifies Yu *et al.*'s notion. Moreover, the architecture proposed by the authors was found to be more scalable and flexible than the RuBee-based system. It relied on the next generation RFID technology which supports reprogramming of RFID tags with dynamic rule encoding scheme. In addition this, the proposed architecture supported extensive and effective monitoring of patients and ensured constant availability of medical information (patients' physiological data, prescriptions, availability of medicines, etc.). However, the authors completely neglected authentication between the RFID readers and tags to ensure the security of critical information at all times. Apart from this, Al-Masri and Hamdi [37] proposed an RFID-based mobile monitoring application in the field of telemedicine. The authors suggested that their application offered a robust distributed system which was capable of monitoring patients' health on a real-time basis. It was formally named as RFIDTrack and it generated alarms for the hospital staff in case of emergency situations. However, the scope of this application was limited within the hospital.

With advancements in the field of communication and telemedicine, technology has gone a step further with implantation of RFID chips inside human body for medicinal purposes. Working in this direction, Werber and Znidarsic [38] proposed an extensive survey related to the potential scope of RFID implantable chips in healthcare industry. Furthermore, the US Food and Drug Administration (FDA) has declared RFID chips to be safe for healthcare purposes [7]. Security and privacy issues linked with implantable devices have been explored in [8].

2.2 Background details about ECC

The foundation of the ECC was laid in the year of 1985 independently, by Neal Koblitz and Victor Miller [24, 39, 40]. It is one of the strongest schemes amongst the other asymmetric approaches such as-RSA, DH, etc. The strength of this technology lies in the fact that, it offers greater security with smaller key sizes. This is because, decrypting the cipher text using the public key in an intractable operation [24] in ECC and is referred to as Elliptic Curve Discrete Logarithm Problem (ECDLP). Table 2.1 shows a comparative view of ECC and RSA in terms of equivalent security and key sizes [24, 39, 40].

The security of ECC lies in the way the operations are performed over the elliptic curve. The standard elliptic curve is based on the two dimensional cartesian coordinate system in

Table 2.1: Comparison between ECC and RSA security with respect to number of bits.

ECC Key Size (Bits)	RSA Key Size (Bits)	Key Size Ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

terms of x and y. The finite field over which the curve is defined, falls into two categories: prime field $GF(P)$ and binary polynomial field $GF(2^m)$ [24, 39, 40]. For the purpose of implementation of this work, elliptic curve operations over the finite binary field $GF(2^m)$ have been considered. The standard equation for the elliptic curve is stated in Eq. (2.1) as follows.

$$y^2 = x^3 + ax + b \tag{2.1}$$

where, coefficients $a, b \in GF(P)$. Equation (2.1) is the simplified version of *Weierstrass* equation that is considered for the computations in cryptographic applications [24, 39, 40]. The actual *Weierstrass* equation over the finite Galios field of order P is stated in Eq. (2.2) as follows.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

Here, a_is are coefficients such that $a_i \in GF(P)$ [39]. The operations that are performed on the elliptic curve form the basis of the underlying security. These operations particularly consists of point multiplication and point doubling. In order to understand these operations, consider the points with their respective cartesian coordinates as depicted in Table 2.2.

Table 2.2: Reference points considered.

Points	Cartesian Coordinates
P	(x_1, y_1)
Q	(x_2, y_2)
R	(x_3, y_3)

2.2.1 Point Addition

Point addition(R) on elliptic curve is governed by the following hypothesis:
Let $P, Q \in E$ such that $P \neq Q$
$\Rightarrow R = P + Q$, where
$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 + x_3) - y_1$
where, $\lambda = (y_2 - y_1)/(x_2 - x_1)$

2.2.2 Point Doubling

Point doubling(R) on elliptic curve is governed by the following conditions:
Let $P \in E$ such that $P \neq -P$
$\Rightarrow R = 2P$, where
$x_3 = \lambda^2 - 2x_1$
$y_3 = \lambda(x_1 + x_3)$
where, $\lambda = (3x_1^2 + a)/2y_1$

2.3 Background details about Petri-net

Petri-nets (PNs) are simple yet powerful analysis tools and different variants of these PNs have been proposed in the literature [41–45]. These are basically used to depict different types of systems with respect to their working, methodology used, security feature evaluation, etc. For example, Mahulea *et al.* [42] used the PN-based scheme to depict the methodology of medical protocols and the resources required in the process of medication at hospitals. Similarly, in this thesis, PN based modeling have been incorporated to clearly depict the methodology used in the authentication protocol and how it counteracts different malicious requests from spoofed servers and tags. The PN scheme clearly depicts the different options available to the system components in the real time scenario and course of action to be executed under different threat scenarios. These scenarios under which the protocol can be compromised are described in Chapter 5.

PNs refer to a place-transition nets, which are depicted in the formal of directed bipartite graphs. These graphs are employed to graphically represent the information flow and control in various distributed systems [43, 45]. In the present era, they are being used to represent various systems and protocols particularly networking protocol [43].

Definition 1: PNs can be defined with respect to the following quadruple [43]:
$PN = (P, T, A, M_0)$
where, $P = \{p_1, p_2, p_3, ...\}$ represents set of places,
$T = \{t_1, t_2, t_3, ...\}$ represents set of transitions,
$A \subset \{P \times T\} \cup \{T \times P\}$ represents set of arcs,
$M_0 = \{m_0, m_1, m_2, ...\}$ represents initial markings where, $m_i = 0, 1, 2, ...; i \in [1, n]$.

These bipartite graphs consist of two kinds of nodes: places and conditions, connected via directed arcs [43–45]. Places represent the various states or conditions of the system and are categorized into two types: input and output places. They are represented graphically in the form of circles. Transitions on the other hand, refer to the events that cause changes in the states of the underlying systems and arcs are represented graphically by solid bars. Arcs refer to the directed lines that connect the previously mentioned entities, i.e., places and transitions. These arcs too can be categorized into two types: Input and Output. While the former are said to connect the input place with its corresponding transition, the latter connects a transition with its respective output place. Former represents the condition or state that needs to be satisfied in order to enable the transition while the later is typically used to represent an occurrence of an event. Places might contain one or several tokens. These tokens are represented graphically by dots. The number of tokens that a particular state contains is referred to as marking. In other words, marking is a vector listing the number of tokens at different places. Arcs have an associated weight or cardinality, referred to as multiplicity (natural number with default value 1). An event is said to be enabled if the number of tokens at input place is equal to the multiplicity of the corresponding arc [43]. These enabled events get fired and tends to change the state of the system. During this process, they tend to deposit tokens at the output place equivalent to the multiplicity of the respective arc. Fig. 2.2 shows the basic representation of PN with various components [45].

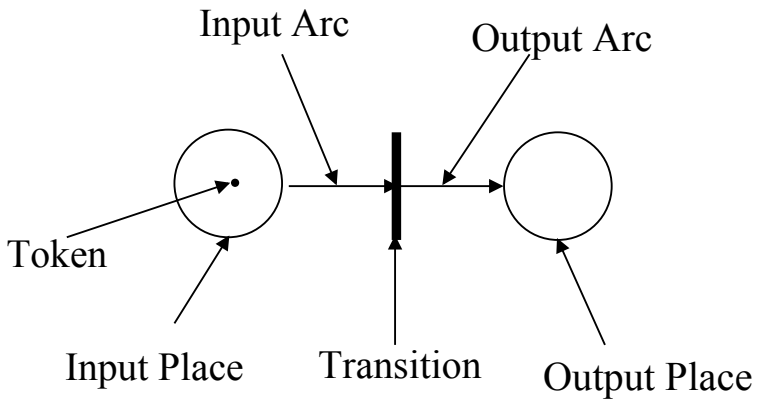


Figure 2.2: Basic Petri-net model comprising of various components.

Chapter 3

Research Motivation and Problem Statement

3.1 Research Motivation

RFID is a cutting edge technology which thrives on radio waves to wirelessly identify and track the tagged objects. Due to its advantages, it has paved its way to many applications ranging from supply chain management to healthcare industry. Incorporation of RFID into healthcare related applications is not new. It has been widely utilized in a number of applications such as-patient monitoring and tracking of laboratory samples, medicines and other related assets [1–3, 6, 8]. However, to the best of our knowledge, none of the existing research proposals have focused on utilizing RFID in transportation systems to provide medical facilities to the patients on move. Thus, this thesis work presents a novel application based on RFID to provide mobile medical facilities. Essentially, the practical realization of this application in the near future possess numerous benefits to mankind.

Due to the wireless channel of communication, RFID is linked with a number of security risks that needs to be tackled before large scale deployment of RFID takes place. Many authentication protocols have been proposed by the researchers in this context. These protocols range from server-less approaches to purely server-based approaches utilising various schemes like public key cryptography, hash functions, pseudo random numbers, etc. Unfortunately, many of the existing protocols and schemes discard the stringent computational requirements of the RFID devices. Additionally, security of the patients' physiological data is of utmost importance in life-critical healthcare applications. Motivated from these challenges, this thesis presents an ECC-based authentication scheme in the context of the proposed RFID-enabled healthcare application.

3.2 Problem Statement

The main contributions of this thesis are summarized as follows.

1. To investigate the current challenges and emerging techniques for implementing an efficient and secure authentication protocol for RFID-enabled healthcare applications.

2. To propose a system model for the potential use of RFID in healthcare domain for providing mobile healthcare facilities.

3. To present an ECC-based secure authentication protocol for RFID-enabled systems.

4. To evaluate the performance of the proposed scheme with respect to various security features and metrics. Additionally, the thesis aims at validating the overall security of the protocol using widely accepted tool-AVISPA.

Chapter 4

The Proposed Scheme

This chapter highlights the proposed RFID-based healthcare application along with its network model, assumptions considered, and working. Additionally, this chapter also provides the detailed working of the proposed ECC-based authentication scheme along with its PN representation.

4.1 The proposed RFID-based healthcare application in vehicular mobile cloud

The proposed RFID-based healthcare application is a novel scheme that aims to enhance the security of the patients on the way. In other words, it aims to provide the necessary first aid facility to the traveling patients at the earliest. The baseline of this model is based to leverage the advantages of the RFID technology with the existing transportation system. Fig. 4.1 described the network model used in the proposed scheme.

4.1.1 Attack Model

The attack model with the respect to the proposed work is described below:

1. An adversary $\mathscr{A}$ may wish to compromise the RFID-based tags or RFID-based readers as the channel between the two parties is insecure.
2. $\mathscr{A}$ can either use passive, active or a combination of both types of methodologies to compromise the tags and readers.
3. In the process of launching attack, $\mathscr{A}$ can either launch rouge tags or readers in the RFID-enabled systems to impersonate the legitimate tags and readers respectively.

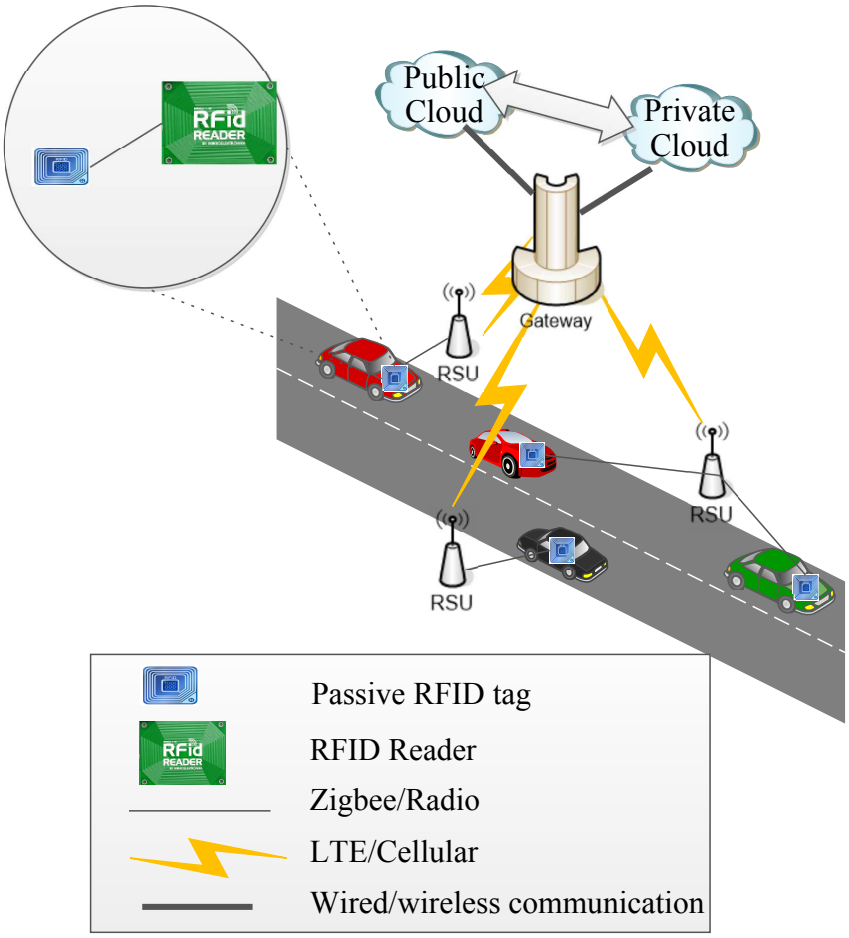


Figure 4.1: Architectural diagram for RFID-enabled healthcare System.

4.1.2 Assumptions Considered

The basic assumptions related to the proposed model are described below:

1. Patients traveling on the roads are to assumed to be wearing RFID-enabled wrist band coupled with Wireless Body Area Network (WBAN).

2. Vehicles and road side units (RSUs) are equipped with low frequency (LF) and ultra high frequency (UHF) RFID-enabled readers respectively.

3. Communication between the RSUs and the central cloud server is supposed to be secure at all times.

4. The communication channel between the RFID-enabled tags and readers is supposed to be insecure and hence, security needs to be incorporated at this level.

4.1.3 Working Methodology

Patients traveling on the road are assumed to be equipped with RFID wrist bands. These wrist bands are passive in nature and are re-programmable. These are capable of capturing the real time physiological information (temperature, blood pressure levels, pulse rate etc.) of the patients by the virtue of WBAN [46–48]. The vehicles are equipped with the low frequency RFID-enabled reader that would capture the physiological information of the patients in its immediate range by using short and medium range communications such as-Bluetooth and WiFi. This capturing process takes place after predefined interval of time and the reader relays this captured information to the central server deployed on the cloud. In the event of accidents, damage, or unavailability of RFID readers inside the vehicles, the RSUs equipped with the same facility would take up the role and hence, provide higher fault tolerance. The readers deployed on the RSU in comparison with their respective counterparts on vehicles are basically UHF readers. Table 4.1 shows a detailed description of the different types of readers and their relative significance with respect to the present scenario [49]. The communication between tags and readers takes place via radio waves operating at different frequencies or IEEE 802.15.4 Zigbee. The communication via Zigbee can take place in multiple hop manner, so it increases the transmission range [50].

Table 4.1: Comparison between types of RFID Frequencies.

Types of RFID Frequencies	**Operating Frequency**	**Reader Range**	**Details**
Low Frequency(LF)	30 KHz to 300 KHz	Up to 10cm	Characterized by shorter read range and slower speed in comparison with other frequency bands. Less susceptible to radio wave interference.
High Frequency(HF)	3 to 30 MHz	10 cm to 1 m	These systems are moderately sensitive to radio wave interference.
Ultra High Frequency (UHF)	300 MHz to 3 GHz	Up to 12 m	Most susceptible to radio wave interference.

Cloud computing paradigm basically provides three types of services: PaaS (Platform as a service), IaaS (Infrastructure as a service) and SaaS (Software as a service). In this case, all the potential applications related to the healthcare domain would be deployed on the cloud infrastructure by virtue of PaaS feature of this technology. This application

suite might consist of various applications, i.e., intelligent expert systems for monitoring the physiological characteristics of patients based on their past history, generating alerts in the form of SMS or calls in case of emergency, checking the staff availability, suggesting medication, details about the nearby hospitals in the vicinity, etc. Here, the cloud platform would play a central role in gathering, maintaining and processing the patients' related data. This central server is supposed to be in synchronization with all the hospitals across the city, wherein the patient's related information would be punched by the hospital staff on a real time basis. It contains present and past information pertaining to patient's illness, prescribed prescription, doctors consulted, emergency contact details etc.

There exists a high speed communication channel (LTE/cellular) between RSUs and cloud platform. This channel is supposed to be secure at all times. Thus, this channel can be utilized by the moving vehicles via vehicle-to-infrastructure (V2I) means of communication. Here, the RSUs simplify act as gateway to the cloud. But in case, the moving vehicles cross the boundaries of RSUs, then the vehicles can collaborate with each other to form vehicular clouds or use vehicle-to-vehicle (V2V) communication (in the form of Zigbee, DSRC, Bluetooth, ultra wide band, etc.) to access various cloud services. The users might be interested in different types of context aware information and services. For example, they might be interested in knowing their present physiological status, availability of a particular doctor at a particular hospital or the prescribed medication. Then in that case, the users will be able to access the cloud services via 3G/4G internet connection with the help of PDAs, smart phones, laptops, etc.

In case, any patient meets any kind of emergency (road accident/sudden attack of specific disease), then his/her respective physiological parameters will get altered and thus, would be sensed by WBAN and would immediately be updated to its relative RFID wrist tag. Then, the reader would read the content of the tag post successful identification and authentication. Finally, reader relays the information to the central server. The server in turn will do the necessary computations and will generate an alarm in case of emergency. This alarm would be generated for the nearest hospital so that the ambulance could reach to the spot as early as possible based on the geographical information received. The server would also relay alert (via automated voice call/SMS) to patient's family member. The entire working of the system is depicted Fig. 4.2.

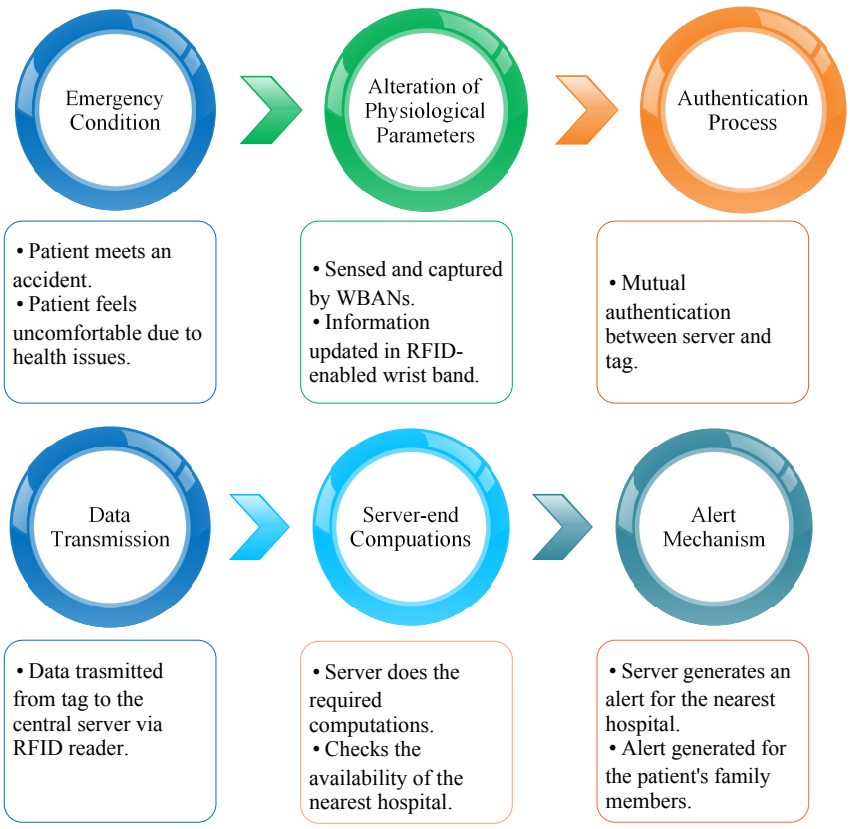


Figure 4.2: Sequence of activities with respect to the proposed deployment of RFID in healthcare domain.

4.2 The proposed ECC-based authentication protocol

In this segment, an efficient and secure mutual authentication protocol with respect to RFID-enabled devices in the field of telemedicine has been explored. In addition to this, the working of the proposed protocol has been elaborated using PN-based approach.

4.2.1 Different Phases

The proposed protocol operates in three phases, i.e., i) initial setup phase, ii) tag authentication phase, and iii) server authentication phase. Various symbols used in this protocol are depicted in the list of symbols. This protocol is based on core ECC operations and additional concatenation and one-way hash operations. ECC is known to be one of the best schemes proposed in the literature so far, for compact, battery operated and computation restrictive devices like RFID [24, 40]. It overpowers the other cryptographic schemes in

terms of security, scalability and performance [24]. On the other hand, use of additional operations with respect to concatenation and one-way hashing makes the approach more resilient against various cyber attacks, e.g., forward secrecy, spoofing attacks, tracking attacks, etc. For the sake of convenience and to make the operations more efficient, elliptic curve over the finite polynomial binary field, i.e., $G(2^p)$ with $p = 163$ has been considered in this work [24, 40].

Phase-1: Initial Setup Phase

The initial phase lays the foundation of all ECC operations in the current system under consideration. RFID enabled tags and the central authentication server (deployed on the cloud), are equipped with all the public parameters of the elliptic curve. These parameters include the following: G, n, P, a, and b. The detailed description about these variables can be found in list of symbols. Apart from this, RFID tags and authentication server are fed with their respective public and private key pairs. Estimation of these key values are based on elliptic curve operations. For private key (x_i) estimation, any random number between the interval $[1, n-1]$ is chosen. After this operation, public key (X_i) is calculated via scalar multiplication of generator point (G) and the corresponding private key (x_i). These operations are depicted in Fig. 4.3. At the end of this phase, following details are maintained by the server and RFID tags respectively:

Server:

- Its own public-private key pairs: x_S and X_S.
- List of all the valid tags in terms of their unique identification number (Id) and public key (X_T).

Tags:

- Its own public-private key pairs: x_T and X_T.
- Public key of the valid server (X_S).

Phase-2: Tag Authentication Phase

This is very crucial step in the process of mutual authentication mechanism between the RFID tags and the server, prior any data transmission. During this step, server authenticates

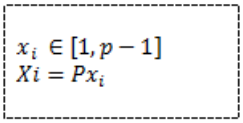


Figure 4.3: Phase-1: Initial setup phase of the proposed authentication protocol.

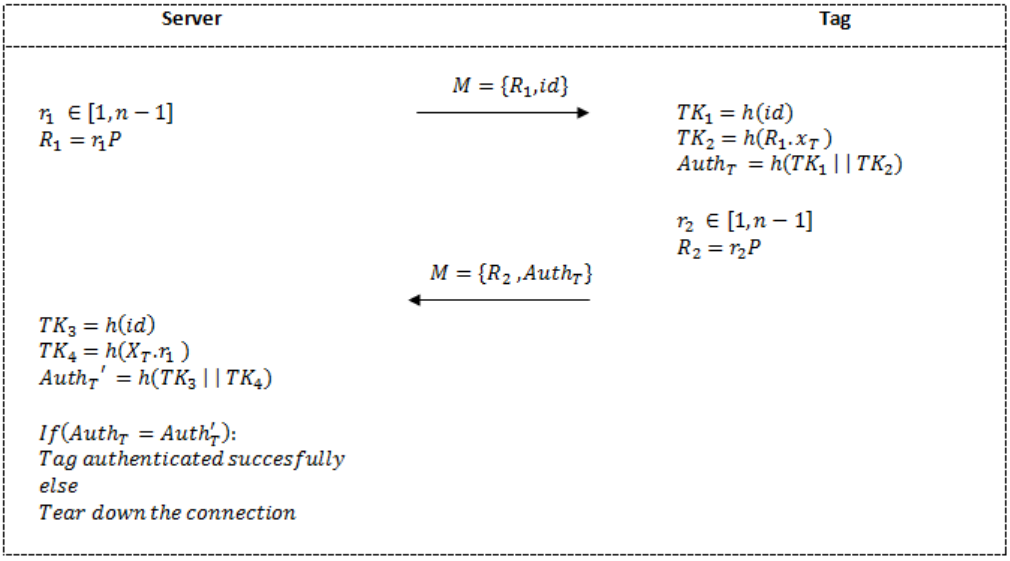


Figure 4.4: Phase 2: Tag authentication phase of the proposed authentication protocol.

the desired tag(s). If authentication is successful, then the connection is continued; otherwise, it is teared down by the central server. The process involved in the tag authentication mechanism is depicted in Fig. 4.4 and elaborated in the followings steps:

- *Step 1:* Server first computes a random number r_1 and then calculates the corresponding R_1 based on scalar multiplication under ECC operations.
- *Step 2:* The server relays the message M containing R_1 and the ID of the tag to be searched.
- *Step 3:* Then, the tag with the corresponding ID computes the $Auth_T$ token and replies back to the server. Computation of this token is elaborated in the below mentioned steps.
- *Step 4:* The tag first computes $TK_1 = h(id)$ (i.e., hash of its own ID). Following this, it carries out an ECC scalar multiplication operation on its own private key x_T and R_1. Computed results of this operation are first hashed and then stored in TK_2.

- *Step 5:* Tag then finally, computes $Auth_T = h(TK_1||TK_2)$. This operation involves simple and efficient concatenation operation followed by one-way hash function.

- *Step 6:* At the same time, tag computes a random number r_2 followed by computing $R_2 = r_2.P$.

- *Step 7:* Then, the tag finally send this computed value of $Auth_T$ along with R_2 to the server for further authentication.

- *Step 8:* Now, the server takes up the role to authenticate the valid tag. This process is initiated by first computing the value of $TK_3 = h(id)$ and then $TK4 = h(X_T.r_1)$. Computation of TK_4 involves a scalar point multiplication of the random number r_1 and tag's public key X_T.

- *Step 9:* After this, $Auth_T{}'$ is calculated and compared with the received $Auth_T$. If both the parameters match, then it signifies that the tag is valid. In case of successful authentication, the server continues with server authentication phase, otherwise; it tears down the ongoing communication with the invalid tag.

Algorithm 1 clearly depicts the sequences of operations under tag authentication phase.

Phase-3: Server Authentication Phase

During this phase, the tag(s) which has been authenticated by the authentication server in the previous phase gets an opportunity to validate the authenticity of the server. Successful authentication by the two parties is followed by data transmission. Unsuccessful authentication process tears down the current connection and hence, inhibits the data communication between the two parties. The process involved in server authentication phase is described in the followings steps and depicted using Fig. 4.5.

- *Step 1:* During this step, the authentication server initially computes the value of TK_5 token. This token is the hash of the scalar multiplication between the R_2 and server's private key x_S.

- *Step 2:* Finally, $Auth_S$ token is computed by the server via $Auth_S = h(TK_3||TK_5)$.

- *Step 3:* Post this the server relays the message M containing $Auth_S$ to the desired tag.

- *Step 4:* Then RFID enabled tag initially computes a token TK_6. This token is computed by taking the hash of $X_S.r_2$ (ECC scalar multiplication of server's public key X_S with r_2).

Algorithm 1 Tag authentication algorithm.

Input: Random numbers r_1 and r_2, id, P, p, a, b, n, X_T, x_T, hash function $h(.)$, concatenation operation $||$

Output: Tag authentication

Assumptions: Both the parties have their respective public and private key pairs and each others public key

Server generates r_1
Server computes R_1 from equation $R_1 = r_1 P$
Message M is relayed from server to RFID tag (R_1 and id)
if ($id =$ actual tag id) **then**
    RFID tag computes $TK_1 = h(id)$
    RFID tag computes $TK_2 = h(R_1.x_T)$
    RFID tag computes $Auth_T = h(TK_1||TK_2)$
    RFID tag generates r_2
    RFID tag computes R_2 from equation $R_2 = r_2 P$
    Message M $(R_2, Auth_T)$ is relayed from tag to server
else
    RFID tag remains silent
end if
Server generates $TK_3 = h(id)$
Server computes $TK_4 = h(X_T.r_1)$
Server computes $Auth_T^{'}$=$h(TK_3||TK_4)$
if ($Auth_T = Auth_T^{'}$) **then**
    Tag authentication successful
else
    Tear down the connection
end if

- *Step 5:* The tag computes $Auth_S^{'}$ token that is based on the concatenation operation of the previously computed TK_1 and TK_6 tokens and finally computes hash of the intermediate result.

- *Step 6:* After this, $Auth_S^{'}$ is calculated and compared with the received $Auth_S$. If both the parameters match, then it signifies that the server is valid; otherwise, server is a spoofed entity.

Algorithm 2 illustrates the detailed working of the this phase.

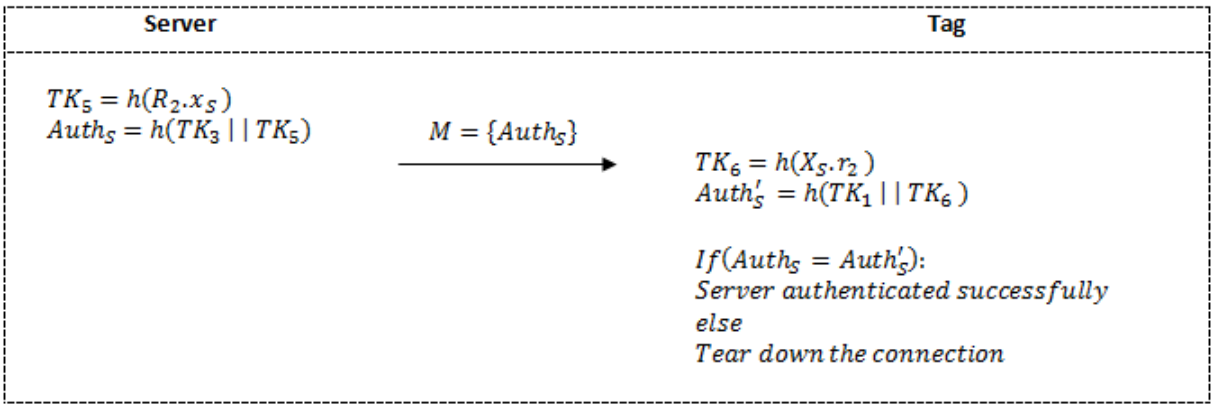


Figure 4.5: Phase 3: Server authentication phase of the proposed authentication protocol.

Algorithm 2 Server authentication algorithm.

Input:random number id, $X_T, P, p, a, b, n, X_s, x_s$, hash function $h(.)$, Concatenation operation $||$

Output: Server authentication

Assumptions: Server has successfully authenticated the tag

1: Server computes $TK_5 = h(R_2.x_S)$
2: Server computes $Auth_S = h(TK_3||TK_5)$
3: Message M $(Auth_S)$ is relayed from server to tag
4: RFID tag computes $TK_6 = h(X_S.r_2)$
5: Server computes $Auth'_S$=$h(TK_1||TK_6)$
6: **if** $(Auth_S = Auth'_S)$ **then**
7: Server authentication successful
8: **else**
9: Tear down the connection
10: **end if**

4.2.2 PN Modelling

PN Model for Tag Authentication Phase

The various symbols used in PN model with respect to tag authentication phase are mentioned in list of symbols. RFID tags in this context have been categorized into two types: legitimate (L) and illegitimate (I). This entire process of tag authentication is shown in Fig. 4.6. Initially tags are in idle place P_{LI}/P_{II}, i.e., not serving any request. Once, these passive tags are activated and queried to initiate request for authentication, then the corresponding transaction T_{LM}/T_{IM} is enabled. This transaction upon firing, deposits a token at P_{LM}/P_{IM}. Now, the respective tag is in a state to generate authentication token $Auth_T$ and to relay this token to AS. The corresponding message generating rate $\lambda_{LT}/\lambda_{LT}$ has Poisson's distribu-

tion in this regard. Hence, transition T_{LQ}/T_{IQ} is fired depositing a token at P_{LQ}/P_{IQ}. This place depicts that the request is submitted and waiting to be serviced by *AS*. *AS* is deployed on the cloud infrastructure and thus, is capable to serve multiple tag request at a time. Thus, *AS* can have multiple tokens such that, the number of tokens depict the number of requests it can handle at a time. Service rate of *AS* ,i.e, μ_A is exponentially distributed. If there is token at P_{LQ}/P_{IQ} place and at least one token at *AS*, then T_{LS}/T_{IS} transaction would be triggered depositing a token at P_{LS}/P_{IS} place. Token at this place signifies that corresponding tag request is being serviced by *AS* for validity. If the validity of the corresponding tag is proven then, T_{NP} transaction is fired depositing a token at P_{NP} and *AS* . This transaction depicts that request was valid and authentication process now moves to the next phase, i.e., Server Authentication Phase depicted $(1)...$. In case, the validity of the tag request fails then, T_{FR} is fired depositing a token at P_{FR} and *AS*. Failure rate λ_A case has exponential distribution. Finally, transaction T_{LI}/T_{II} takes the tag to its respective idle place P_{LI}/P_{II}.

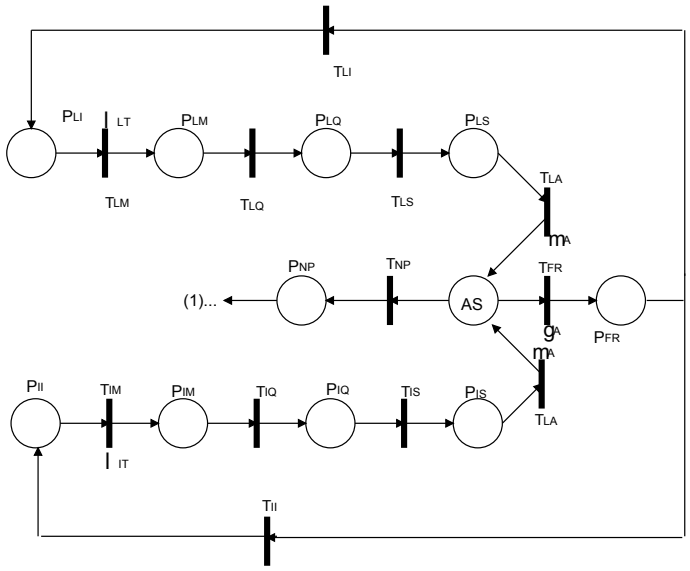


Figure 4.6: PN model for tag authentication phase.

PN Model for Server Authentication Phase

AS in this context have been categorized into two types: real(R) and spoofed(S). This entire process of authentication is depicted in Figure 5. Message generating rate of servers is depicted by $\lambda_{RS}/\lambda_{SS}$ and has Poisson's distribution whereas, the service and failure rate of RT are exponentially distributed and depicted by μ_R and γ_R respectively. Initially, servers are in idle place P_{RI}/P_{SI}, i.e., not serving any request. Once, these servers are queried/ pro-

grammed to initiate request for authentication then, corresponding transaction T_{RM}/T_{SM} is enabled. This transaction upon firing, deposits a token at P_{RM}/P_{SM}. Now, the respective server is in a state, to generate authentication token $Auth_S$ and to relay this token to RT. Hence, transaction T_{RQ}/T_{MQ} is fired depositing a token at P_{RQ}/P_{MQ}. This transaction depicts that the request is submitted for authentication and is waiting to be serviced by RT. RFID tags are resource constrained devices and capable to serve only one request at a time. Thus, the RT can have maximum of one token. If there is token at P_{RQ}/P_{MQ} place and one token at RT, then T_{RS}/T_{MS} transaction would be triggered depositing a token at P_{RS}/P_{MS} place. Token at this place signifies that corresponding server request is being serviced by RT for validity. If the validity of the corresponding server is proven then T_{CA} transaction is fired depositing a token at P_{NP} and RT depicting that request was valid and authentication process has successfully completed. In case, the validity of the tag request fails then, T_{FR} is fired depositing a token at P_{FA} and RT. Then, respective server is taken back to idle place P_{RI}/P_{MI}.

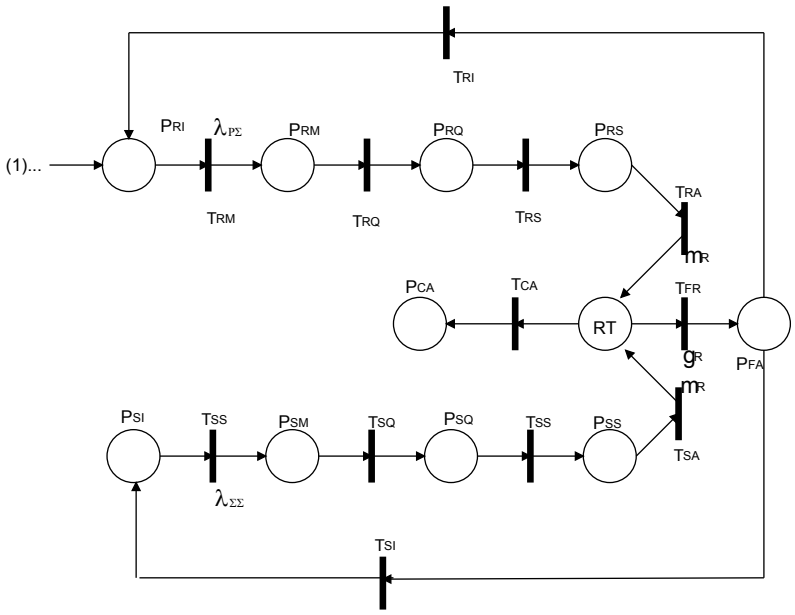


Figure 4.7: PN model for server authentication phase.

Chapter 5

Security Evaluation

In this chapter, detailed security evaluation of the proposed ECC-based authentication protocol has been presented. Different scenarios where the integrity of the proposed protocol could be violated and the system could be under the threat condition have been analyzed. The results indicate that the proposed protocol is capable enough to resist the below mentioned attacks.

5.1 Supports Mutual Authentication

The proposed authentication scheme supports the concept of mutual authentication. This is justified from the fact that in phase-2, i.e., tag authentication phase, the desired tag generates $Auth_T$ token. This token can only be generated with the knowledge of tag's private key x_T . Likewise, during phase-3, i.e., server authentication phase, the central server needs to generate the AuthS token. This token cannot be computed without the knowledge of server's private key x_S. This clearly depicts that, only the authentic parties have the capability to validate and authenticate each other. Moreover, the computation of private keys by the adversary $\mathscr{A}$ from the corresponding knowledge of public key is an intractable approach referred to as ECDLP [24, 39, 40].

5.2 Resists Eavesdropping Attack

The proposed protocol is resilient against eavesdropping attack on the insecure channel between RFID-enabled readers and tags. This implies that even if the $\mathscr{A}$ sniffs the ongoing communication between centralized server and the RFID-enabled tags, $\mathscr{A}$ would not be

able to decrypt any information in order to serve her malicious intent because the intermediate tokens computed in the different phases either require the secret keys x_S/x_T or pseudo random number r_1/r_2. Moreover, the use of ECC and one-way hash operations in the underlying authentication scheme makes it pretty impossible to compute the private key from the available information, i.e., R_1, R_2, $Auth_S$ and $Auth_T$. Thus, the eavesdropping attack would not yield any fruitful information to $\mathscr{A}$.

5.3 Supports Anonymity

The proposed protocol supports the concept of anonymity. This is simply proven from the fact that in each run random numbers (r_1 and r_2) are generated which are further used in estimation of $Auth_S$ and $Auth_T$ tokens. Here, $Auth_T = h(h(id)||h(R_1.x_T))$, $Auth_S = h(h(id)||h(R_2.x_S))$, $R_1 = r_1P$ and $R_2 = r_2P$. Hence, decrypting these tokens is a very difficult task since, they have been computed with the help of ECC, concatenation and one-way hash operations. Moreover, the use of random numbers in each run, makes the corresponding tokens to yield different values in each run.

5.4 Resists Replay Attack

The protocol gracefully resists the replay attack. This is evident from the fact that in each sub authentication phase, the intermediate tokens ($AuthT$, $AuthS$) are computed with help of R_1 and R_2, where $Auth_T = h(h(id)||h(R_1.x_T))$, $Auth_S = h(h(id)||h(R_2.x_S))$, $R_1 = r_1P$ and $R_2 = r_2P$. These random numbers ensure that these token yield different values in every run and thus, the proposed protocol drops and discards the replayed messages.

5.5 Resists Tracking Attack

In case, $\mathscr{A}$ is able to track any tag, then it would be possible for $\mathscr{A}$ to track and reveal information related to a particular patient(s). However, the proposed protocol even prevents these location tracking attacks on the RFID tags. Let us suppose, $\mathscr{A}$ has extracted the identification number ID of a tag from the channel. However, this information alone is not sufficient for the $\mathscr{A}$ to guess or intercept the subsequent communication between the server and numerous tags. The interception of the messages relayed during phase-2 and

phase-3 between the tags and server is not possible due to underlying ECC, one-way hash, and concatenation operations.

5.6 Resists Server Spoofing Attack

In the proposed scheme, the adversary $\mathscr{A}$ would not be able to spoof the server. This is evident from the fact, $\mathscr{A}$ cannot generate $Auth_S$ token without server's private key, i.e., x_S to bypass phase-3. Moreover, the computation of the private key from the knowledge of the publicly available ECC parameters is an intractable approach [24, 40].

5.7 Resists Tag Masquerading/ Spoofing Attack

In order to spoof any RFID-enabled tag(s) and bypass the authentication process, $\mathscr{A}$ requires x_T of the actual tag. This is required in order to successfully generate $Auth_T$, where $Auth_T = h(TK_1||TK_2)$, $TK_1 = h(id)$, $TK_2 = h(R_1.x_T)$, $R_1 = r_1P$. The knowledge of the public key of the tag is not enough to compute the private key since the underlying process is based on ECC operations.

5.8 Supports Forwards Secrecy

Forwards secrecy refers to the fact that previous communications and messages relayed between the server and tags should not be revealed, even if $\mathscr{A}$ acquires the present information of the system i.e., public-private key pairs or/and random numbers. This is evident from the fact that, during each run to authenticate the entities, pseudo random numbers are generated based on ECC operations. These random numbers make the intermediate tokens acquire different values in each run. Thus, the present knowledge acquired by $\mathscr{A}$ with respect to present random numbers and private-public key pairs would not be helpful to retain the previously transmitted information. Thus, our proposed scheme withstands forward security.

5.9 Resists Cloning Attack

Cloning is the process of impersonating the legitimate entities (i.e., RFID tags) involved in the system. During the initial setup phase, private and public keys are computed and assigned to each legitimate tag. In the entire process of mutual authentication, the only static information available to the adversary in the clear text is ID field. This information by no means is sufficient to reveal the private keys of the tags to successfully clone them. Moreover, if one tag is compromised than this would not lead other tags at risk of being compromised, since every tag has unique public-private key pairs and ID.

Chapter 6

Performance Evaluation

RFID-enabled devices particularly RFID tags have limited computational resources. Moreover, few tags are dependent on readers to perform their respective tasks [23,32]. Thus, it is highly important to analyze the proposed scheme with respect to various parameters. Thus, this chapter deals with the security features and performance comparison of the proposed scheme with the existing schemes in detail. In addition to this, the protocol proposed in this thesis has been formally evaluated with the help of AVISPA.

6.1 Comparison with other schemes

6.1.1 Performance comparison

For the purpose of evaluating the effectiveness of the proposed scheme, 163-bit NIST elliptic curve has been considered having finite binary field, i.e., $F(2^{163})$. In addition to this, the hash operations are performed using SHA-1 which gives an output hash of 160 bits. In [35], Godor et al. computed the computational time for performing different operations on a 5 MHz RFID tag. Authors estimated that it takes around 0.064 sec, 0.00553336 sec and 0.00012623 sec to perform ECC-based scalar multiplication, AES-based encryption or decryption, and SHA-1 based hash operation respectively on the tag. These result values from [35] have been considered in the following segment for performance comparison of the protocol. Essentially, three parameters have been considered for performance evaluation as mentioned below.

Storage Requirements

RFID tags relatively have reduced storage capabilities in comparison to RFID readers, thus, for the purpose of evaluating the proposed protocol, the storage requirements at the tag level

have been considered [7]. The storage requirements are expressed in terms of protocol related data that needs to be stored in the tag's memory. This data refers to public keys, private keys and curve parameters required during the authentication process. The private key in this case refers to tag's private key x_T (163 bits). On the other hand, public key comprises of tag's and server's public key (X_T and X_S) which require 163 bits each for storage. Apart from storing these keys, RFID tag also stores the E parameters for performing ECC operations which require 163 bits in total. Table 6.1 presents the comparison of the proposed scheme with existing schemes in regard of the storage requirements.

Computational Cost

The computational cost of the scheme has been evaluated with respect to the number of major operations such as-ECC scalar point multiplications, one-way hashing functions, encryption and decryption operations. Other operations such as-pseudo random number generation, concatenation, XOR operations, etc. have not been considered for since, they are very light and comparatively require less computational resources. Table 6.1 illustrates the comparison of the proposed protocol with different schemes in terms of computational cost.

Communication overhead

The total communicational cost has been estimated by considering the number of rounds and total size of messages shared during the authentication mechanism. Table 6.1 provides a detailed comparison of the proposed authentication scheme with the others.

6.1.2 Security features comparison

Table 6.2 represents the comparison of different security features with respect to various authentication protocols against the proposed protocol. The detailed comparison with respect to various attacks such as-spoofing, tracking, replaying, etc., clearly depict that the proposed ECC-based protocol is the most secure in comparison with others.

Table 6.1: Performance comparison with different authentication protocols.

	Ours	**Batina *et al.* [36]**	**Goder *et al.* [35]**	**Liao *et al.* [16]**	**Chao [14]**
I. Memory Requirements					
Private key	163 bits	163 bits	163 bits	163 bits	163 bits
Public key	326 bits	326 bits	326 bits	326 bits	326 bits
Public parameters	163 bits	163 bits	163 bits	163 bits	163 bits
Total	82 B	82 B	82 B	82 B	82 B
II. Computational cost					
ECC scalar multiplications	3	2	3	5	2
Hash operations	5	0	0	0	2
Encryption operations	0	0	1	0	0
Total	0.193 sec	0.128 sec	0.197 sec	0.32 sec	0.129 sec
III. Communicational overhead					
Number of Rounds	3	3	4	3	3
Data transferred	105 B	82 B	82 B	82 B	126 B

Table 6.2: Security feature comparison of different authentication protocols

	Ours	**Batina *et al.* [36]**	**Goder *et al.* [35]**	**Tian-tian *et al.* [13]**	**Liao *et al.* [16]**	**Chao [14]**
Mutual Authentication	✔	✗	✔	✔	✗	✗
Anonymity	✔	✗	✔	✗	✔	✗
Forward Secrecy	✔	✗	✗	✗	✔	✗
Tag Spoofing	✔	✗	✔	✗	✗	✗
Server Spoofing	✔	✗	✔	✗	✗	✗
Location Tracking	✔	✗	✔	✔	✗	✗
Replay	✔	✔	✗	✔	✔	✔

✔: Represents that protocol is secure against the said attack
✗: Represents that protocol is insecure against the said attack

6.2 Formal security verification using AVISPA

This segment presents the formal security verification of the proposed ECC-based authentication protocol. This verification has been carried out with the help of Automated Vali-

dation of Security Protocols and Applications (AVISPA). The results obtained through the analysis indicate that the proposed protocol is resilient against passive and active attacks.

AVISPA is a popular tool which is widely used for security evaluation of internet protocols [51]. The tools performs robust analysis of protocols in an automated manner with the help of inbuilt back-ends namely-OFMC, CL-AtSe, SATM and TA4SP. The tool accepts the protocol specification in the form of role oriented HLPSL language. Detailed information about AVISPA's working and HLPSL can be found in [51].

For the purpose of implementation of this work, tag and server authentication phases have been specified using HLPSL. The formal security analysis of this work has been done using two agents. These agents are namely- *rfidtag (T)* and *rfidserver (S)*. The specifications of these roles are depicted in Fig. 6.1 and 6.2 respectively. The implementation of these specifications are described as follows. Initially, S receives a start signal and changes its state from 0 to 1. After this, S generates a random number and sends the first message to T in the form of $M = (R_1, id)$ using $Snd()$ function. Agent T receives this message via the public channel using $Rcv()$ function. Then, T does the necessary computations and sends $M = (R_2, Auth_T)$ to S. Finally, S generates the last token in the server authentication phase and sends $M = (Auth_S)$ to T for cross validation.

In these specifications, the threat model for the security analysis has been defined using $channel(dy)$. This denotes that the intruder's model is Dolev-Yao threat model [51] in which the intruder has the ability to sniff and modify the messages communicated over the insecure link between S and T.

Fig. 6.3 depicts role of session used in the implementation. The session instantiates the agents used in the specification, with certain parameters. As shown in the figure, agents namely-$rfidserver$ and $rfidtag$ have been instantiated with seven arguments for each. Apart from this, environment and goal specifications are highlighted in Fig. 6.4. This portion of the HLPSL specifications contains the global constants and one or more sessions. Different secrecy and authentication goals of this analysis have been specified in the last part of this specification, i.e., goal.

The simulation results of the proposed protocol are shown in Fig. 6.5. The results have been obtained by analyzing the protocol specification written in HLPSL using the web interface of AVISPA. The results indicate that the proposed authentication protocol is secure against active and passive attacks as specified in OFMC back-end.

From the above mentioned results and comparisons, its is evident that the proposed authentication scheme outperforms the existing authentication schemes in terms of resistance against different security attacks. Moreover, the proposed scheme also provides acceptable memory, computational and communicational cost while providing higher security.

```
role rfidserver (S,T: agent,
% Public keys
            Xt, Xs: public_key,
% H is a hash function
            H: hash_func,
% Sending and receiving channels
            Snd,Rcv: channel(dy))
played_by S
def=
  local State   : nat,
        R1, R11, P, R2,R22, Autht,
Tk3,
        Tk5, Auths,Id: text,
        F: hash_func
  const r1, r2, id, xtt,
xss,server_tag_r11,
  tag_server_r22,
tag_server_autht,
  server_tag_auths,server_tag_id:
protocol_id

  init  State := 0
  transition
%Tag Authentication Phase
   1. State = 0
      /\ Rcv(start)
      =|>
      State' := 1
      /\ R1':= new()
      /\R11':= F(R1'.P)
      /\ Snd({R11'.Id}_Xt)
      /\ secret(R1', r1, S)
      /\witness(S, T, server_tag_id,
Id)
      /\witness(S, T, server_tag_r11,
R11')
%Server Authentication Phase
   2. State = 1
      /\ Rcv(R22'.Autht')
      =|>
      State':= 2
      /\Tk3':= H(Id)
      /\Tk5':= H(F(R22'.inv(Xs)))
      /\Auths':=H(Tk3'.Tk5')
      /\Snd(Auths')
      /\secret(inv(Xs), xss, S)
      /\witness(S, T,
server_tag_auths, Auths')
end role
```

Figure 6.1: Role specification for RFID server in HLPSL in context of the proposed protocol.

```
role rfidtag (S,T: agent,
% Public keys
            Xt, Xs: public_key,
% H is a hash function
            H: hash_func,
% Sending and receiving channels
            Snd,Rcv: channel(dy))
played_by T
def=
  local State   : nat,
        R1, R11, P, TK1, TK2, Autht,
        Auths, R2, R22,Id : text,
        F: hash_func
  const r1,r2, id, xtt, xss,
server_tag_r11,
  tag_server_r22,tag_server_autht,
  server_tag_auths,server_tag_id  :
protocol_id

  init  State := 0
  transition
%Tag Authentication Phase
   1. State = 0 /\ Rcv({R11'.Id}_Xt)
      =|>
      State' := 1
      /\request(S, T, server_tag_r11,
R11')
      /\request(S, T, server_tag_id, Id)
      /\ TK1' := H(Id)
      /\ TK2' := H(F(R11'.inv(Xt)))
      /\ Autht' := H(TK1'.TK2')
      /\ R2' := new()
      /\R22' := F(R2'.P)
      /\ Snd(R22'.Autht')
      /\ secret(inv(Xt), xtt, T)
      /\ secret(R2', r2, T)
      /\witness(T, S, tag_server_r22,
R22')
      /\witness(T, S, tag_server_autht,
Autht')
%Server Authentication Phase
   2. State = 1 /\ Rcv(Auths')
      =|>
      State' := 2
      /\request(S, T, server_tag_auths,
Auths')
end role
```

Figure 6.2: Role specification for RFID tag in HLPSL in context of the proposed protocol.

```
role session(S,T: agent,
Xt, Xs: public_key,
H: hash_func)
def=
  local SS, RS, ST, RT:
channel (dy)
composition
     rfidserver
(S,T,Xt,Xs,H,SS,RS)
    /\rfidtag
(S,T,Xt,Xs,H,ST,RT)
end role
```

Figure 6.3: Session specification in HLPSL in context of the proposed protocol.

```
role environment()
def=
  const s, t   : agent,
  xt, xs: public_key,
  h   : hash_func,
  f   : hash_func,
  p : text,
  r1,r2, id, xtt, xss,
server_tag_r11,
tag_server_r22,
tag_server_autht,
server_tag_auths :
protocol_id

  intruder_knowledge=
{s,t,xs,xt,h,f,p}
  composition
    session(s,t,xs,xt,h)
end role

goal
 secrecy_of r1,r2, xtt, xss
 authentication_on
server_tag_r11,
tag_server_r22,
 tag_server_autht,
server_tag_auths,server_tag_i
d
end goal

environment()
```

Figure 6.4: Goal and environment specification in HLPSL in context of the proposed protocol.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS

BOUNDED_NUMBER_OF_S
ESSIONS
PROTOCOL
  /home/avispa/web-interface-
computation/./tempdir/workfile
wfpMW8PHWY.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s
  visitedNodes: 2 nodes
  depth: 1 plies
```

Figure 6.5: Results obtained using AVISPA in context of the proposed protocol.

Chapter 7

Conclusion and Future Scope

7.1 Conclusion

RFID is becoming more and more ubiquitous, so its privacy and security concerns are becoming challenging these days. Thus, implementing security into RFID-enabled healthcare applications is a challenge keeping in view the resource constrained nature of RFID tags. In this thesis, a light weight and an efficient ECC-based authentication protocol has been proposed for a typical healthcare application based on RFID. The proposed protocol provides a mean to successfully authenticate the server and tags prior to any communication. The entire process of authentication is based on efficient ECC, concatenation, and one-way hash operations. Furthermore, Petri-net based models have been formulated for tag and server authentication phases. In addition to this, detailed security analysis of the proposed protocol has been done in comparison with the existing protocols. Moreover, AVISPA tool has been used for its formal security evaluation. The performance evaluation based on different metrics depicts that the scheme is practical enough to be implemented in healthcare industries to enhance reliability and safety.

7.2 Future Scope

In the future, we would apply the RFID authentication scheme in smart grid environment. We further aim to enhance the security aspect of the protocol. We will also try to provide the test bed implementation of the scheme. We will make use of the higher level PN modeling schemes such as-colored petri nets (CPNs), object oriented petri nets (OOPNs), etc. [41,42] in order to validate the security features of the protocol.

Bibliography

[1] S. L. Ting, S. K. Kwok, A. H. C. Tsang, and W. B. Lee, "Critical elements and lessons learnt from the implementation of an RFID-enabled healthcare management system in a medical organization," *Journal of Medical Systems*, vol. 35, pp. 657–669, Dec. 2009.

[2] S. F. Wamba, A. Anand, and L. Carter, "A literature review of RFID-enabled healthcare applications and issues," *International Journal of Information Management*, vol. 33, no. 5, pp. 875–891, 2013.

[3] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and privacy in RFID and applications in telemedicine," *IEEE Communications Magazine*, pp. 64–72, Apr. 2006.

[4] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[5] X. Yu, X. Xia, and X. Chen, "Design and application of rubee-based telemedicine data acquisition system," in *IEEE/ACIS 10th International Conference on Computer and Information Science (ICIS)*, May 2011, pp. 365–370.

[6] M. Chen, S. Gonzalez, V. Leung, Q. Zhang, and M. Li, "A 2G-RFID-based e-healthcare system," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 37–43, Feb. 2010.

[7] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "An elliptic curve-based mutual authentication scheme for RFID implant systems," in *5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)*. Elsevier, 2014, pp. 198–206.

[8] C. Camaraa, P. Peris-Lopeza, and J. E. Tapiadora, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272–289, 2015.

[9] S. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC based RFID authentication protocol," in *12th IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS*, Oct. 2008, pp. 219–225.

[10] S. I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, and T. Nakajima, "Secure and efficient tag searching in RFID systems using serverless search protocol," *International Journal of Security and Its Applications*, vol. 2, no. 4, pp. 57–66, 2008.

[11] T. Y. Won, J. Y. Chun, and D. H. Lee, "Strong authentication protocol for secure RFID tag search without help of central database," in *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC*. IEEE, 2008, pp. 153–158.

[12] H. Jialiang, X. Youjun, and X. Zhiqiang, "A hash-based RFID search protocol for mobile reader," *International Journal of Hybrid Information Technology*, vol. 7, no. 8, pp. 139–150, 2014.

[13] Y. Tian-tian and F. Quan-yuan, "A security RFID authentication protocol based on hash function," in *International Symposium on Information Engineering and Electronic Commerce*, 2009, pp. 804–807.

[14] L. V. Chao, L. I. Hui, M. A. Jianfeng, and Z. H. A. O. Meng, "Security analysis of two recently proposed RFID authentication protocols," *Frontiers of Computer Science*, vol. 5, no. 3, p. 335, 2011.

[15] Y.-Y. Chen, J.-C. Lu, S.-I. Chen, and J.-K. Jan, "A low-cost RFID authentication protocol with location privacy protection," in *Fifth International Conference on Information Assurance and Security,IAS*, vol. 2, Aug. 2009, pp. 109–113.

[16] Y.-P. Liao and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Networks*, vol. 18, pp. 133 – 146, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870513000243

[17] R. Peeters and J. Hermans, "Attack on liao and hsiao's secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," Cryptology ePrint Archive, Report 2013/399, 2013, Available: http://eprint.iacr.org/, [Accessed: May 2015].

[18] T. Deursen and S. Radomirovic. Attacks on RFID protocols (version 1.1). Technical Report. Available: https://eprint.iacr.org/2008/310.pdf, [Accessed: Apr. 2015].

[19] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Proceedings of the 7th International Conference on Cryptology and Network Security*. Springer-Verlag, 2008, pp. 149–161.

[20] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol," in *IEEE International Conference on RFID*, Apr. 2008, pp. 97–104.

[21] N. Druml, M. Menghin, A. Kuleta, C. Steger, R. Weiss, H. Bock, and J. Haid, "A flexible and lightweight ECC-based authentication solution for resource constrained systems," in *17th Euromicro Conference on Digital System Design (DSD)*, Aug. 2014, pp. 372–378.

[22] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75–94, 2014.

[23] M. Farash, "Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 2, pp. 987–1001, 2014.

[24] "An elliptic curve cryptography (ECC) primer: Why ECC is the next generation of public key cryptography," The Certicom Catch the Curve White Paper Series, Jun. 2004, Available: https://www.certicom.com, [Accessed: Apr 2015].

[25] T. V. Le, M. Burmester, and B. D. Medeiros, "Universally composable and forward-secure RFID authentication and authenticated key exchange," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*. ACM, 2007, pp. 242–252.

[26] D. N. Duc and K. Kim, "Defending RFID authentication protocols against DoS attacks," *Computer Communications*, vol. 34, no. 3, pp. 384–390, 2011.

[27] A. X. Liu and L. A. Bailey, "PAP: a privacy and authentication protocol for passive RFID tags," *Computer Communications*, vol. 32, no. 7-10, pp. 1194–1199, 2009.

[28] G. Tsudik, "YA-TRAP: Yet another trivial RFID authentication protocol," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE, 2006, pp. 1–4.

[29] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337–340, 2007.

[30] U. Mujahid, M. Najam-ul Islam, and M. A. Shami, "RCIA: A new ultralightweight RFID authentication protocol using recursive hash," *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.

[31] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Computer Communications*, vol. 34, no. 3, pp. 391–397, 2011.

[32] Y. Chen, J.-S. Chou, and H.-M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, pp. 2373–2380, 2008.

[33] T. Cao, P. Shen, and E. Bertino, "Cryptanalysis of some RFID authentication protocols," *Journal of Communications*, vol. 3, no. 7, pp. 20–27, 2008.

[34] T.-C. Yeh, C.-H. Wu, and Y.-M. Tseng, "Improvement of the RFID authentication scheme based on quadratic residues," *Computer Communications*, vol. 34, no. 3, pp. 337–341, 2011.

[35] G. Gódor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations," in *IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*. IEEE, 2010, pp. 650–657.

[36] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public-key cryptography for RFID-tags," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops*. IEEE, 2007, pp. 217–222.

[37] E. Al-Masri and M. Hamdi, "RFID-based approach for monitoring patients health inside hospitals," in *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering*. Springer, 2015, pp. 607–613.

[38] B. Werber and A. Žnidaršič, "The use of subcutaneous RFID microchip in health care-a willingness to challenge," *Health and Technology*, pp. 1–9, 2015.

[39] S. Bala, G. Sharma, and A. K. Verma, "Optimized elliptic curve cryptography for wireless sensor networks," in *2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC)*. IEEE, 2012, pp. 89–94.

[40] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[41] Y. Xu and X. Xie, "Modeling and analysis of security protocols using colored petri nets," *Journal of Computers*, vol. 6, no. 1, pp. 19–27, 2011.

[42] C. Mahulea, L. Mahulea, J.-M. Garcia-Soriano, and J.-M. Colom, "Petri nets with resources for modeling primary healthcare systems," in *18th International Conference System Theory, Control and Computing (ICSTCC)*. IEEE, 2014, pp. 639–644.

[43] O. C. Ibe and K. S. Trivedi, "Stochastic petri net models of polling systems," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 9, pp. 1649–1657, 1990.

[44] R. Entezari-Maleki, K. S. Trivedi, and A. Movaghar, "Performability evaluation of grid environments using stochastic reward nets," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 2, pp. 204–216, 2015.

[45] M. Malhotra and K. S. Trivedi, "Dependability modeling using petri-nets," *IEEE Transactions on Reliability*, vol. 44, no. 3, pp. 428–440, 1995.

[46] Y.-C. Chen, H.-M. Sun, and R.-S. Chen, "Design and implementation of wearable RFID tag for real-time ubiquitous medical care," in *IEEE Topical Conference on Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS)*. IEEE, 2014, pp. 25–27.

[47] G. E. Jan, C.-C. Sun, L.-P. Hung, Y.-S. Jan, and S.-H. Weng, "Real-time monitor system with RFID localization for seniors," in *IEEE 17th International Symposium on Consumer Electronics (ISCE)*. IEEE, 2013, pp. 75–76.

[48] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID technology for IoT-based personal healthcare in smart spaces," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 144–152, 2014.

[49] The different types of RFID systems. Impinj. Available: http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems, [Accessed: Apr 2015].

[50] N. F. B. I. Gulcharan, H. Daud, N. M. Nor, T. Ibrahim, and E. T. Nyamasvisva, "Limitation and solution for healthcare network using RFID technology: a review," *Procedia Technology*, vol. 11, pp. 565–571, 2013.

[51] “AVISPA v1.1 user manual,” Automated Validation of Internet Security Protocols and Applications, Jun. 2006, Available: http://www.avispa-project.org/package/user-manual.pdf, [Accessed: May 2015].

Publications

SCI/SCIE Publications

1. N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications*, pp. 1-17, Feb. 2015, doi:10.1007/ s12083-015-0332-4.
2. K. Kaur, N. Kumar, and M. Bansal, "An ECC-based authentication protocol for RFID-enabled Systems," *Wireless Personal Communications*, under review.

International/National Conference Publications

1. K. Kaur and N. Kumar, "Smart grid with cloud computing: Architecture, security issues and defense mechanism," *9th International Conference on Industrial and Information Systems (ICIIS)*, Dec. 2014, ABV-Indian Institute of Information Technology and Management, Gwalior, India.

Video Presentation Link

`https://youtu.be/6RffLsV953o`