ACCESS MANAGEMENT IN UBIQUITOUS e-HEALTHCARE ENVIRONMENT

By

Muhammad Umair Aslam

A thesis submitted to the Faculty of Information Security Department, Military College of Signals, National University of Science and Technology, Pakistan in partial fulfillment of the requirements for the degree of Masters in Information Security

May 2018

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere, except the literature review, that has been used in 'A Survey of Authentication Schemes in Telecare Medicine Information Systems' journal paper publication in 'Journal of Medical Systems, Springer US' .

Muhammad Umair Aslam

DEDICATION

”In the name of Allah, the most Beneficent, the most Merciful”

I dedicate this thesis to my parents, sister, brother and my teachers.

ABSTRACT

e-Healthcare is an emerging field that provides mobility to its users. The protected health information of the users are stored at a remote server (Telecare Medical Information System) and can be accessed by the users at anytime. Many authentication protocols have been proposed to ensure the secure authenticated access to the Telecare Medical Information System. These protocols are designed to provide certain properties such as: anonymity, untraceability, unlinkability, privacy, confidentiality, availability and integrity. They also aim to build a key exchange mechanism, which provides security against some attacks such as: identity theft, password guessing, denial of service, impersonation and insider attacks. This thesis reviews these proposed authentication protocols and discusses their strengths and weaknesses in terms of ensured security and privacy properties, and computation cost. The schemes are divided in three broad categories of one-factor, two-factor and three-factor authentication schemes. Inter-category and intra-category comparison has been performed for these schemes and based on the derived results we propose a hybrid solution based on the roles of the users. The propose solution ensures security and privac properties for physicians and ensure easiness for patients. The research also presents future research directions and recommendations that can be very helpful to the researchers who work on the design and implementation of authentication protocols.

ACKNOWLEDGMENT

First and foremost, I would like to thank Allah Almighty for providing me courage and motivation during the thesis to handle all challenges in pleasing manner.

My utmost debt of gratitude is to my supervisor Dr. Baber Aslam and Co-supervisor Astt Prof Mian Muhammad Waseem Iqbal. It has been an honor to study under their supervision. I appreciate all their generous contributions of time, ideas, and guidance for the improvement of my research work.

I offer my deepest gratitude to my committee members Dr. Mehreen Afzal and Lec Waleed Bin Shahid who have put their prodigious efforts throughout the thesis phase with their knowledge, expertise and valuable suggestions. They have provided full support, mentorship and continuous assistance despite their utmost busy commitments. I am highly thankful to Dr. Abdelouahid Derhab, Dr. Haider Abbas, Dr. Kashif Saleem, Dr. Mehmet Orgun and Dr. Monis Akhlaq who have been guiding me throughout my research work and have helped increase my knowledge. I am also thankful to Syed Shah Fahd, Muhammad Awais and Muhammad Sadiq Khan for sharing their knowledge, insights and providing valuable feedback.

Lastly, I would like to thank my family for all their love and encouragement. For my parents who raised me with a love of science and supported me in all my pursuits. And most of all for my loving, supportive and encouraging sister and brother whose faithful support during the final stages of my degree is so appreciated. Thank you it would not have been possible without you.

TABLE OF CONTENTS

LIST OF FIGURES

LSIT OF TABLES

Chapter 1

INTRODUCTION

1.1 Introduction

Chapter 1 presents the introduction, architecture and operations of e-Healthcare services. It also contain brief description of motivation of the chosen research area, problem statement, objectives and methodology of research, contributions and arrangement of the research work.

1.2 e-Healthcare Architecture and Operation

With the advancement of technology, healthcare services can be provided remotely, where sensors measure the patient's condition, feed the data to mobile devices such as PDAs or cell phones and from where it is transmitted to heath provider's Telecare Medicine Information System (TMIS). TMIS has provided the leverage of movement to both patients and physicians. Patients can login to the system to check their medical records, get test results and history of prescribed medicines. Physicians can check the history of prescribed medicines, test results and on the basis of those can always change the prescription [1, 2].

As the communication between a cell phone/smart card and TMIS takes place on the public Internet, the whole system is vulnerable to threats associated with open Internet [2]. Privacy and especially anonymity is the biggest hurdle in implementation of an e-Healthcare system globally. In e-Healthcare, a patient registers with the TMIS to access health services remotely. Then, he/she needs to login to the server, which requires proper authentication so that the services are

not abused [2, 3, 4, 5].

Many authentication mechanisms have been proposed starting from a simple password to two-factor and three-factor authentication schemes. The first remote computer authentication scheme was proposed by Lamport [6]. The scheme was very simple and required only the username and the password from the users to access the system. The authentication schemes, which were proposed for a remote computer/machine, tended to protect the user password and did not consider the privacy and anonymity, which are the main concerns for a user in the e-Healthcare environment. Later on, more complex and secure authentication schemes were proposed.The first two-factor authentication scheme was proposed by Hwang [7] in 1990, and early in the 21^{st} century, the three-factor authentication schemes were proposed. In e-Healthcare, all authentication schemes start with the registration phase where the user registers remotely with the TMIS. After successful registration, the user needs to be authenticated before being granted access to the TMIS. The one-factor authentication protocols provide easiness as the user only needs to remember his/her password for the authentication purposes. Two-factor authentication requires smart card in addition to the ID and password, which decreases the user's comfort level. In three-factor authentication, the user needs to provide his/her biometric information in addition to smart card, ID and password.

The authentication schemes consist of the following phases:

- *Registration Phase:* In this phase, the user registers with the TMIS by providing personal information and identity. A password can be chosen at a later stage or at the registration phase and it is subject to change after the first login.
- *Login and Authentication Phase:* In this phase, the user accesses the services provided by the TMIS by giving his/her identity.
- *Password Change Phase:* This phase is introduced so that the user can update his/her pass-

word regularly, which minimizes the probability of attacks due to using the same password.

- *Revocation Phase:* In this phase, the user credentials are revoked in case of any compromise.

A basic architecture of e-Healthcare is described in Figure 1.1. Bio-sensors measure the patient's physiological conditions and feed that information to a smart phone/ PDA, from where they are transmitted to health provider's servers using the public Internet. The storage server holds the patient's Protected Health Information (PHI), and access to PHI is granted under the implemented policies by the policy server and only after the successful authentication from the authentication server. The area of interest is shown inside the red block, which contains the user, physician, authenticating server and the TMIS. In e-Healthcare, the patient accesses the PHI for monitoring his/her health condition, the physician accesses for prescription and pharmacist accesses it to verify the prescribed medicines [8]. In emergency situations an ambulance can also be called to provide timely first aid to the patient before reaching the hospital. Research and development wing deeply analyzes the sensors input for behavioral analysis to predict emergency conditions.

1.3 Motivation

e-Healthcare is an emerging field of science which focuses on providing healthcare facilities to all, specially to those who do not have physical access to medical facilities. The architecture provides a framework where medical condition of a patient can be measured remotely all the time and treated accordingly. As a new field of science it has a vast scope of research and demands the attention of the research community for its continuous evaluation so that it can gain the users trust as an alternate where users do not have physical access to medical facilities. To be globally accepted by the users the domain requires that researchers explore the weakness in the proposed architecture, propose solutions for identified weaknesses and finally make the architecture effi-

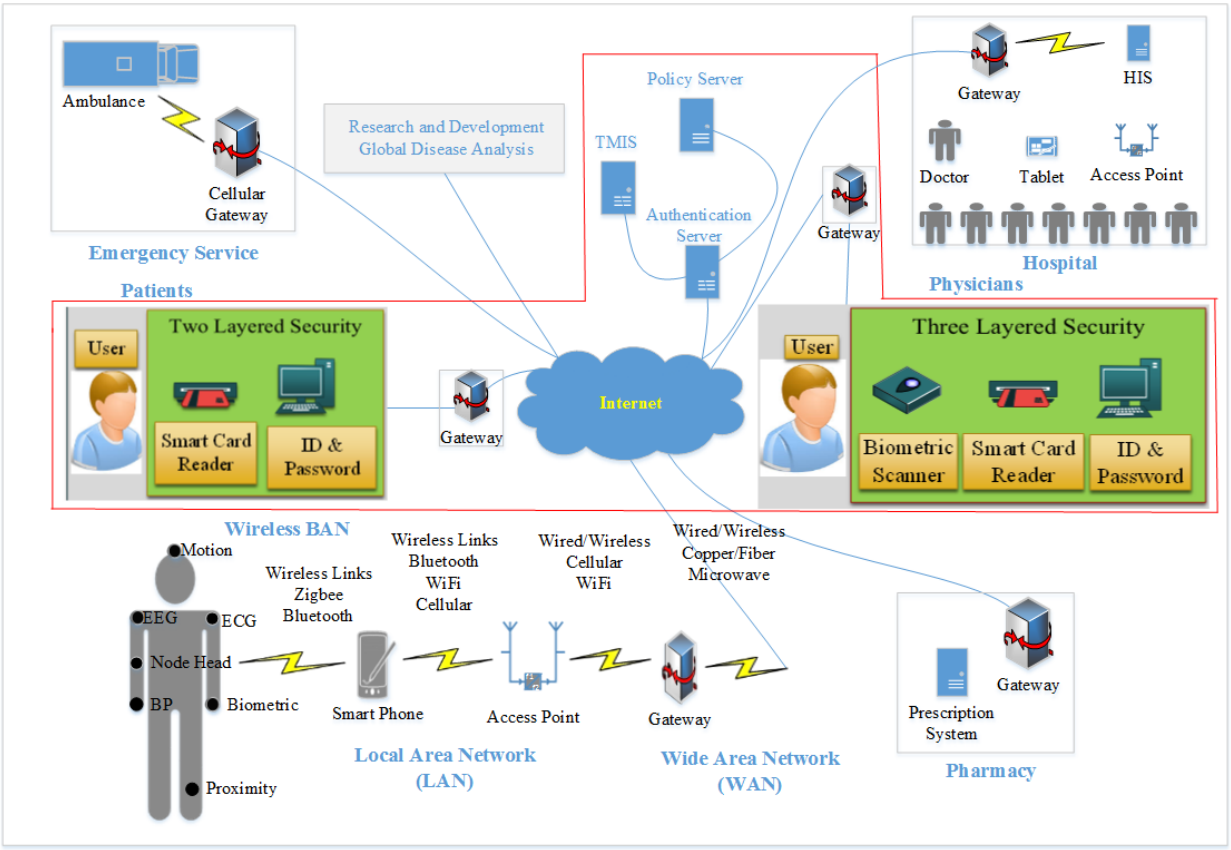

Figure 1.1: e-Healthcare Architecture

cient and secure for the users.

1.4 Problem Statement

To access the services provided by the e-Healthcare provider, users need to register with the service provider so that the service provider can authenticate and differentiate between legitimate users. To make the registration and authentication process secure, many researchers have proposed authentication schemes. Some proposed two-factor authentication schemes, whereas others have presented three-factor authentication schemes. Both have their advantages over one another but none is found secure enough to be advocated. The proposed schemes do not differentiate between patients and physicians and offers the same level of security for both, whereas both have different roles and impact in the e-Healthcare architecture. So there is a need for an authentication scheme that addresses the above mentioned issues.

1.5 Objectives

The objectives of the research are as following:

1. Design a criteria for authentication schemes
2. Evaluate existing authentication schemes based on the designed criteria
3. Evaluate different category schemes and highlight their advantages as well as their weaknesses
4. Propose a solution that can take the benefits of different categories and can also differentiate between patients and physicians
5. Propose a secure authentication scheme that can also provide privacy and anonymity to its users
6. Propose an authentication scheme that meets and satisfy the designed criteria

7. Propose future research directions based on the present research work

1.6 Research Methodology

Descriptive, associational, qualitative and problem oriented methodologies have been adopted while conducting the research. Several research and surveys papers have been studied and authentication schemes have been evaluated qualitatively. Several statistical data sources have been analyzed to get the holistic picture of the stated problem. Few practical implementations of the e-Healthcare systems and implemented standards have also been studied for practical approach. The focus of the research is to find the solution for the stated problem and meet the objectives defined in objective section.

1.7 Contribution

As e-Healthcare is a new service delivery mechanism in the field of healthcare services, it has comparatively vast scope for contribution than other established fields. Contribution of our research work in the field of e-Healthcare is described as follows:

1. We have designed a performance criteria for authentication schemes, the criteria serves as a guideline for the researchers in designing their authentication schemes for the e-Healthcare.
2. We have evaluated several well-known authentication schemes against the proposed performance matrix and ranked them accordingly, which provides a holistic view of the existing authentication schemes and also highlights the areas of improvement in those authentication schemes.
3. We have evaluated and highlighted the advantages and disadvantages of different authentication categories, which helps the researchers choosing a category for designing their authentication schemes.

4. We have proposed a role based novel solution, that takes the benefits of all categories to meet the user expectations from the e-Healthcare services.
5. We have proposed two different authentication schemes, one for the patients and the other for the physicians. The security analysis proves that the proposed schemes meet and satisfy the proposed performance criteria designed for the evaluation of authentication schemes.

1.8 Thesis Organization

The thesis is arranged in following chapters:

Chapter 1 presents the introduction of the research, Chapter 2 presents the preliminaries and Chapter 3 presents performance metrics. Chapter 4, Chapter 5, and Chapter 6 cover the evaluation of one-factor, two-factor and three-factor authentication schemes respectively. Chapter 7 presents the proposed hybrid model of authentication schemes, Chapter 8 presents the security analysis of the authentication schemes presented in Chapter 7 and finally, Chapter 9 presents the conclusion of the research work and also presents guidelines for future research directions based on the research work.

1.9 Conclusion

Chapter 1, presented the introduction, architecture and operations of e-Healthcare services. It also contained brief description of motivation of the chosen research area, problem statement, objectives and methodology of research, contributions and arrangement of the research work.

Chapter 2

PRELIMINARIES

2.1 Introduction

Chapter 2 is divided in three sections. Section 2.1 contains the introduction of the chapter. Section 2.2 briefly reviews the concepts of security and privacy properties e.g anonymity, untraceability, unlinkability, pseudonymity, session key verification, forward secrecy and efficient password update. Section 2.3 reviews adversary attacks on authentication schemes e.g. password guessing attack, replay attack, privileged insider attack, denial-of-service attack, impersonation attack, stolen verifier attack and stolen smart card attack. Section 2.4 briefly describes the cryptographic algorithms, e.g. one-way hash function, bio-hashing, Rivest-Shamir-Adleman and elliptic curve cryptography. Finally, Section 2.5 presents the conclusion of the chapter.

2.2 Security and Privacy Properties

Any given authentication scheme should ensure the following security and privacy properties:

2.2.1 Anonymity

This property refers to the protection of the user's real identity and ensures privacy. It ensures that the user's real identity is not revealed, and does not travel on the communication channel [9]. The adversary and the server cannot learn the real identity of the user from the authentication messages [10].

2.2.2 Untraceability

This property ensures that the server or the adversary cannot trace the communication back to the user [10], i.e., keeping the user anonymous.

2.2.3 Unlinkability

This property ensures that any transmitted data by the user cannot be linked to the user by any means [11, 12], e.g., medical records possessed by the TMIS cannot be linked to the relevant user of the TMIS.

2.2.4 Pseudonymity

This property ensures that the true identity of the user does not travel on the communication in any circumstances. False or fake identity of user is used to access the TMIS [11, 12] instead of the true identity to keep the user anonymous.

2.2.5 Session Key Verification

A session key is a symmetric key, which is used to secure the communication between two parties and shared after successful authentication. The verification of the session key ensures the legitimacy of communicating parties [13, 14].

2.2.6 Forward Secrecy

This is a property of a secure communication protocol, which ensures that compromise of the long term keys does not compromise the past session keys and hence the whole communication [15, 16, 17].

2.2.7 Efficient Password Change

This is a property of an efficient communication protocol where an old password is required and matched when changing the password [18]. The password is not sent on the communication channel in plain [19]. The password is always verified at the end-user before communicating it to the server.

2.3 Attacks on Authentication Schemes

The adversary exploits the vulnerabilities present in an authentication protocol by using different attacks. One of the basic objectives of the researchers while proposing an authentication protocol is to make sure that the proposed protocol is resilient against these attacks.

2.3.1 Password Guessing Attack

This attack is possible when an adversary gets a copy of the encrypted password from the communication channel or from the smart card. In this attack, the adversary guesses thousands of passwords per second and matches them with the captured one until the guessing operation succeeds [20]. The adversary can also use precomputed password dictionaries to enhance this process substantially [21]. Online password guessing has limited scope as applications do not allow infinite attempts and block the malicious user after a few unsuccessful attempts, whereas in offline password guessing there is no such limitation [22]. The successful execution of this attack will enable the attacker to access the information on TMIS, compromising the confidentiality and user privacy.

2.3.2 Replay Attack

In a replay attack, the adversary eavesdrops the communication channel and captures the authentication messages. The authentication messages, which contain the user response against the server's challenge are maliciously replayed to get access and abuse the TMIS [23, 24, 25, 26]. Replay attacks can also affect the availability of the system as the attacker can send replay messages in bulk and the target system processes every message before it can make any decision.

2.3.3 Privileged Insider Attack

This attack is perpetrated by a person who has an authorized system access [27, 28, 29]. An insider can steal the user's sensitive information from the TMIS, and hence user's privacy, anonymity and untraceability can easily be compromised by the attacker [29, 30]. An insider who has privileged system access can also affect the integrity of the information.

2.3.4 Denial-of-Service Attack

In this attack, an attacker sends a huge amount of replay or false packets to the server to keep it busy and prevent it from providing services to legitimate users [31]. As the server processes each packet (legitimate or illegitimate) resources such as memory, processing power and bandwidth are consumed. Under such an attack, the false messages consume all the resources of the server to its full capacity and therefore the server cannot process any further requests (legitimate or illegitimate), [32, 33, 34, 35]. This attack compromises the availability of the TMIS by depriving the the access to its legitimate users.

2.3.5 Impersonation Attack

In an impersonation attack, the adversary steals the identity of one of the legitimate parties to get access to the TMIS [36, 37]. In a server impersonation attack, the adversary assumes the identity of the server and tricks a legitimate user to get his/her secret information that can later be used to access the TMIS [38]. In the user impersonation attack, the adversary assumes the identity of the legitimate user to abuse services provided by the TMIS [38]. The successful execution of this attack will enable the attacker to get access the information on TMIS, compromising the confidentiality and user privacy.

2.3.6 Stolen verifier attack

In this attack, the attacker steals the verification data from the server of a current or past successful authentication sessions [39, 40]. The adversary uses the stolen data to generate authentication messages and sends it to the server. If the server accepts the authentication messages, the adversary impersonates as a legal user. The successful execution of this attack will enable the attacker to get access the information on TMIS, compromising the confidentiality and user privacy.

2.3.7 Stolen Smart Card Attack

In a stolen smart card attack, the adversary extracts the information from the stolen smart card by monitoring its power consumption during different operations [41, 42, 43, 44, 45, 46]. Information can also be extracted by monitoring the time it takes to perform a certain operation. This attack challenges the implementation of the encryption algorithm and not the algorithm itself. The successful execution of this attack will enable the attacker to get access the information on TMIS, compromising the confidentiality and user privacy.

2.4 Cryptographic Functions

2.4.1 One-Way Hash Function

A cryptographic one-way hash function takes input of an arbitrary length string and maps it to a fixed length output.

$$H(x) = y$$

Where $x = \{0,1\}^*$ and $y = \{0,1\}^n$, that is, *x* a binary string of an arbitrary length and y is a binary string of fixed length *n*. A cryptographic hash function satisfies the following properties.

1. Given $m \in x$: it is hard in polynomial time to find the input *m* for the given output y.
2. It is hard to find the input $m^{'} \in x$ such that $m^{'} \neq m$ and $H(m) = H(m^{'})$.
3. It is hard to find a pair $(m, m^{'}) \in x * x$ such that $H(m) = H(m^{'})$, where $m \neq m^{'}$.

2.4.2 Bio-Hashing

Biometric information has a great significance in authentication mechanisms. Biometric-based authentication schemes, provide access to the remote system on the basis of the user's biometric (fingerprint, retina scan, face, palmprint etc.) information. Generally, the user biometric information do not remain the same for each session [47, 48], which leads that the user faces a high rate of false rejection. Jina et al. [49] addressed this issue and proposed a set of user specific compact codes, also known as bio-hashing, produced from user specific biometric features and tokenised pseudo-random number. Later, Lumini and Nanni [50] proposed the improvement of bio-hashing, and other improvement efforts include [51, 52, 53].

2.4.3 Rivest-Shamir-Adleman (RSA)

RSA is a public key cryptosystem designed by Rivest Shamir and Adelman [54] in 1978. Components of RSA are *N, p, q, e and d.* The security of a system is based on the complexity of the factorization problem, i.e, the adversary is unable to factorize the composite number *N* in polynomial time. RSA cryptogram uses two separate but mathematically linked keys, public and private keys. Public key is used to encrypt the messages, whereas private key is used to digitally sign the message. RSA is widely used for signing messages such as in Internet browsers [55], where a secure connection is required over an insecure channel. If public key is used to encrypt the message, then private key will be required to decrypt it. RSA ensures confidentiality, integrity, authenticity and non repudiation [56, 57, 58].

2.4.4 Elliptic Curve Cryptography (ECC)

Due to large computation problems in RSA, ECC was proposed by Neil Kobleitz [59] and Miller [60] in 1985. ECC was designed for resource constrained environments. It offers equivalent security to RSA with far smaller key size, and hence reduces the processing overhead. ECC is widely used in cell phone applications as it requires less storage space, RAM and processing as compared to other cryptograms [61, 62, 63, 64, 65]. It is worth mentioning that not all the elliptic curves are secure, some of them are highly vulnerable, so it is necessary to verify the curves before using them. Elliptic curves are described by cubic equations similar to those used for ellipses and also known as Weierstrass equation.

$$E : Y^2 + axy + by = X^3 + cx^2 + dx + e$$

Where *a, b, c, d, e* are real numbers and *x* and *y* take on values in the real numbers. The above equation can be reduced to the following form:

$$E : Y^2 = X^3 + ax + b$$

Security of ECC relies on point scalar multiplication in additive group. For a point *P* of primitive order on curve $E_p(a, b)$ such that $Q = dP$, where *Q, P* remains public and *d* is a private parameter. It is relatively easy to determine *Q* given *d* and *P* but it is very hard to determine *d* given *Q* and *P* and this is called the discrete logarithm problem for elliptic curves.

2.5 Conclusion

This chapter 2, presents basic concepts of security and privacy properties, adversary attacks and cryptographic algorithms used in the reviewed authentication schemes, which helps the reader in understanding the next chapters, where we have used these basic concepts for the evaluation of proposed authentication schemes. This chapter provides the basic foundation to understand the research work, presented by other authors while proposing their authentication schemes and also presented by the thesis author in this research work.

Chapter 3

PROPOSED PERFORMANCE METRICS

3.1 Introduction

Chapter 3 is divided in three sections. Section 3.1 contains the introduction of the chapter. In Section 3.2, the proposed performance metrics have been designed for the evaluation of authentication schemes. Computation cost, communication cost, delay, user efficiency, server efficiency, resistance against known attacks, ensured security, privacy properties, security index and mobility are the main components of designed metrics against which authentication schemes can been evaluated. Finally, Section 3.3 contains the conclusion of chapter 3.

3.2 Proposed Performance Metrics

The performance of any given authentication scheme can be evaluated in terms of its resilience against known attacks, security and privacy properties it ensures, computation cost, delay, communication cost, user easiness etc. The performance metrics we use in this thesis are given in [66, 67, 68, 69, 70, 71]. The authentication scheme must be resilient against all known attacks e.g. impersonation attack, replay attack, offline password guessing attack, privileged insider attack, stolen verifier attack, denial-of-service attack [68] etc. The protocol must provide the desired properties, e.g., forward secrecy, revocation mechanism for stolen or lost smart cards, efficient password update, user privacy, session key verification [72, 73] etc. In addition, we propose a new performance metric, called security index, defined as the number of security and privacy

properties ensured by the scheme. An authentication scheme with higher security index ensures more security and privacy properties, and hence is more favorable for practical use.

As e-Healthcare provides mobility to its users [74, 75, 76, 77], the authentication may take place between a resource constrained device and the TMIS [78, 79, 80, 81], so the protocol should be light enough in terms of computation and communication (bandwidth) to support resource constrained devices [82, 83]. For this purpose, we compare the authentication schemes in terms of:

- *User computation:* It measures the number of operations performed by the end-user's host during the login and authentication phase.
- *Server computation:* It measures the number of operations performed by the server during the login and authentication phase.

The efficiency of the schemes presented in Table 5.2 and 6.2 refers to their computation cost. It only includes the computation cost the scheme incurs during the login and authentication phase, as the computation cost of the registration phase occurs only once and it also does not impact on the overall efficiency of the given scheme. The authentication protocol should be easy for users to use [84, 85, 86]. It should support flexibility to remember passwords [87] and does not require ideally anything else for the authentication purpose. Surveys [86, 88] have shown that the usability index of an authentication scheme drops while increasing the user interaction. Generally, users do not feel comfortable in providing their biometric information [89], hence three-factor authentication schemes are the least comfortable in terms of user easiness [88]. Healthcare services are critical and require urgent attention, which makes the delay factor more important.

In one-factor authentication schemes, the user provides his/her username along with the password and the TMIS grants or rejects the access request on the basis of the provided input. In

two-factor authentication schemes, the user inserts his/her smart card into the smart card reader, the TMIS authenticates the smart card, and then the user proceeds further as for the one-factor authentication schemes. In three-factor authentication schemes, the user proves his/her identity first by providing biometric information and proceeds further as for the two-factor authentication schemes.

It can be observed that two-factor authentication schemes have added delay as the user interacts with the TMIS twice, once for the authentication of the smart card and then for the verification of the username and password. Three-factor authentication schemes incur more delay [90] as the user interacts with the TMIS three times, once for biometric information, then for the smart card and finally for the username and password. Computation cost of an authentication scheme is directly proportional to delay, as each computation operation requires time, which adds delay to the scheme and contributes to the overall latency of the scheme. This thesis reviews the performance of the proposed protocols on the basis of the provided security and privacy properties, the user computation cost, and evaluates the authentication methods on the basis of user easiness, computation cost, communication cost, delay, ensured security and privacy properties, and their ability to facilitate mobility. The above mentioned performance metrics are summarized in Table 3.1 for better understanding.

Each authenticating method has its own advantages over the others, a tradeoff that has to be accounted while choosing any one of them. Our proposed hybrid solution, presented in Chapter 7, Section 7.6, focuses on user easiness, comfortableness and available resources when authenticating a user, as we have proposed and presented a two-factor authentication scheme in Chapter 7, Section 7.7. On the contrary, the hybrid solution focuses on complexity and enhanced security when authenticating a physician, as we have proposed and presented a three-factor authentication scheme in Chapter 7, Section 7.6 that adds user biometric information to two-factor authentication

scheme. The hybrid solution offers different authentication methods to patients and physicians as both have different access levels to the TMIS [91, 92]. Authenticating the user with an easy, comfortable and less resourced authenticating method has some disadvantages, similarly, authenticating a physician with a complex and enhanced security method also has some disadvantages. The advantages and disadvantages of different authentication methods are discussed in detail in 7, in Section 7.6, and summarized in Table 7.2.

Metric	Role
Resistance against known attacks	It indicates whether the authentication scheme is able to defend against all known attacks or not e.g., impersonation attack, replay attack, offline password guessing attack, privileged insider attack, stolen verifier attack, denial-of-service attack [68].
Ensured security properties	It indicates whether the security properties are ensured or not by the authentication scheme, e.g., forward secrecy, revocation mechanism for stolen or lost smart cards, efficient password update and session key verification [72, 73].
Ensured privacy properties	It indicates whether the privacy properties are ensured or not by the authentication scheme, e.g., anonymity, untraceability, unlinkability and pseudonymity [9, 10, 11, 12].
Computation cost	It evaluates the efficiency of the scheme during the login and the authentication phase in terms of the number of operations performed by the user's device and the server [82, 83, 93].

Table 3.1: Performance metrics

Metric	Role
Communication cost	It evaluates the efficiency of the authentication scheme with respect to the amount of data exchanged between the user and the server and takes three qualitative values: low, medium, and high [67, 82, 83].
Delay	It evaluates the efficiency of the scheme in terms of latency incurred during the login and authentication phase, and takes three qualitative values: low, medium, and high [67].
User easiness	It evaluates the efficiency of the scheme with respect to level of user interaction and easiness during the login phase, and takes three qualitative values: low, medium, and high [84, 85, 86].
Security Index	It represents the rank of the authentication scheme, which is defined as the number of security and privacy properties any authentication scheme ensures.
Mobility	It indicates the level of mobility, which is allowed by the authentication scheme, and takes three qualitative values: low, medium, and high [74, 75, 76, 77].

Table 3.1: Performance metrics

3.3 Conclusion

In this chapter 3, we have have proposed a performance metrics for the evaluation of authentication schemes. The performance metrics is based on the the computation cost, communication cost, delay, user efficiency, server efficiency, resistance against known attacks, ensured security,

privacy properties, security index of the proposed schemes, and also their ability to provide mobility to their users. The proposed metrics serves as a basic foundation for the researchers in proposing an authentication scheme for e-Healthcare. It also provides a criteria to the researchers for the evaluation of already proposed scheme.

Chapter 4

ONE-FACTOR AUTHENTICATION SCHEMES

4.1 Introduction

In Section 4.2, one-factor authentication schemes have been evaluated. Pros and cons of authentication schemes have been described in detail and later in the section a detailed analysis is also given for the one-factor authentication schemes. The last Section 4.4 contains the conclusion of the chapter based on the evaluation of the proposed one-factor authentication schemes.

4.2 One-Factor Authentication Schemes

4.2.1 Lamport's scheme

Leslie Lamport [6] proposed the first ever remote system authentication scheme in 1981. The scheme was proposed to solve the two basic problems of that time. (1) An intruder can access the remote system physically and extract or modify the user credentials. (2) The adversary can also get the credentials by eavesdropping on the communication channel.

The first problem was addressed by taking the hash of the password before storing it in the system. Now, the user will have to send his/her password in plain to the remote system. The latter will compute the hash of the password and compare it with the stored one. If the two hashes are equal, then access is granted to the user. Otherwise, access is denied. An intruder can still get the credentials by eavesdropping as they are sent in clear. As the credentials are sent in clear, the scheme also does not provide the privacy and anonymity to the user.

Lamport addressed the 2^{nd} problem by proposing a sequence of passwords, in which the next session password depends on the last session password used. This sequence is only known to the user and to the server. The scheme was good enough to solve the stated problems but it burdened the server as too many passwords are required for each user, and one password for each session. The scheme is vulnerable to insider threat, as the password sequence is stored at the remote side in plain form and can be used by the insider to abuse the services. At the failed attempt, the the scheme does not inform the user whether the sequence or the password is incorrect.

4.2.2 Shimizu's scheme

Shimizu [94] proposed improvements to the Lamport scheme [6]. The latter [6] incurs an additional burden as it computes the hash function *n* times if the user logs for the n^{th} time. Shimizu's scheme [94] only computes the hash function once and attaches the last authenticated hash as a reference to prove its authenticity. The strength of the scheme lies in the one-way hash function as it cannot be reversed to obtain the input password.

The scheme claims to resist against the eavesdropping, as the hash of the password is transmitted on the channel instead of the plain password. The scheme is vulnerable to replay attack as it does not verify the freshness of the messages, an adversary can replay the previous authenticated messages to achieve access to the remote system. The scheme is vulnerable to insider threat, as the password and the last authenticated hash are stored at the remote side and can be used to abuse the services.

4.2.3 Harn's scheme

Harn [95] proposed a public key cryptography based dynamic password scheme that uses digital signatures to bind the user identity with its respective password. The user registers and receives

a password from the registration authority. In the login phase, the digital signatures are used to determine the legitimacy of the user. Harn proved in [6] that the user will have to acquire another set of passwords after exhausting all the given passwords at the registration time. He also proved that the remote system will have to apply the hash function several times for authentication, which compromises the efficiency of the scheme.

He proposed his scheme [95] to address the dictionary attack problem on the encrypted password file stored on the remote system. His proposed scheme does not store any password in any form in the remote system and the user password is dynamic, i.e., it changes after every login.

4.2.4 Steiner's scheme

Steiner proposed [96] a service-based model for an authentication scheme. In his scheme, to access any service, the user needs to identify and prove its identity. When a user requires services, his/her identity is established by presenting a ticket to the server along with a proof that the ticket belongs to the desired user and not to a stolen one.

Authentication through Kerberos has three phases. In the first phase, the user obtains the credentials to be used for accessing the remote system. In the second phase, the user requests authentication for a specific service, and in the third and final phase, the user presents the given credentials to the authenticating server and the access to the desired service is granted. This scheme does not verify the freshness of the messages, so the adversary can replay the previous session's authenticated messages to impersonate as a legitimate user to get access to the remote system.

4.2.5 Bellovin et. al scheme

Bellovin et al. [97] proposed a password-based authentication scheme that uses both symmetric and asymmetric cryptography. This scheme was presented to thwart the dictionary attack due to

weak passwords chosen by the users. The scheme encrypts the randomly generated public key or session key with the shared secret to start the session and exchange information on insecure channel. The shared secret is the password in this scheme, known also as *Encrypted Key Exchange,* or *EKE.* The scheme is vulnerable to insider threat as password is known to both parties: the user and the server. The scheme does not ensure user anonymity as user name is sent in clear along with encrypted key. The scheme is also vulnerable to replay attack as both parties do not verify the freshness of the received messages.

4.2.6 Haller et al. scheme

Haller et al. [98] proposed a one-time password system to solve the growing problem of eavesdropping. He stated that his scheme does not store or retain any kind of information about the password on both sides, the password is never sent on the network, and it resists the modification and replay attack. The security of the scheme lies in the 64 bit one-time password secret generated at the end-user. In the login phase, the user presents his/her identity and the remote system issues a challenge and the sequence number of the one-time password, which also works as the seed. The user enters the sequence followed by the one-time password related to that sequence.

4.2.7 Gwoboa's scheme

Gwoboa [99] proposed an authentication scheme and argued that the user name or ID must also be protected along with the password to improve the overall security of the scheme. In this scheme, one-way function is used to hide the password and one-way trapdoor function is used to hide the identity of the user. The scheme maintains polynomial table of the ID and password to resist against the brute force attack. This is one of the first scheme, which tried to hide user ID to increase the workload of the attacker. The scheme does not verify the freshness of the

authentication messages and hence, vulnerable to replay attack. As the server stores the secret information, an insider attack is also possible.

4.3 Analysis

One-factor, password-based authentication schemes appeared when Internet was very limited in efficiency, and the ability and resources of the adversary were also very limited. The primary problem, which researchers tried to solve is the storage of the password or verification table. A password or verification table was maintained at the remote server so that the user's given credentials can be matched and the access can be granted. An adversary can get access to the server and can compromise the stored credentials. In early solutions, researchers proposed to store encrypted passwords instead of the plain ones. After doing this, the adversary cannot learn the credentials but he/she can delete, modify or replace them with another set of encrypted passwords. This problem leads the researchers to propose solutions where the remote computer does not have to store a verifier table to authenticate users. Researchers proposed schemes where authentication can be performed without the verifier table. The secondary problem was eavesdropping where an adversary listens to the communication, captures user password and uses it to get access to the remote server. As the password is transmitted in plain, researchers proposed to send an encrypted one instead of the plain one. Encrypted passwords failed to resist against dictionary attacks as the length and the strength of the password was used to be weak at that time. Then researchers proposed solutions where a sequence and its associated encrypted password would be sent to a remote computer and that password would never be used again. This approach was secure but it put a burden on communication as it is known that at the early days of Internet, the communication channel capacity was also an issue. After the emergence of public key cryptography, researchers proposed solutions based on the user-signature.

All the one-factor password-based authentication schemes were proposed to thwart the password storage, eavesdropping and unauthorized resource usage problems. Anonymity, privacy, and untraceability were never taken into consideration. Comparison of one-factor authentication schemes is presented in Table 4.1 and in Figure 4.1. It can be seen in the table that all one-factor authentication schemes fail to provide adequate security and if the password is compromised then there is no other protection to save the server from the abuser. Most of the one-factor authentication schemes suffer from impersonation attack as the adversary can replay the previous authentication messages to impersonate as legitimate user.

The one-factor authentication schemes only aim to hide the password and transmits the username in plain, which compromises the privacy and anonymity. The computation cost for most of the one-factor authentication schemes is approximately the same, as all of them take only the hash of the password at both ends. Table 4.1 refers to the number of security and privacy properties ensured by the scheme. From Table 4.1, it is evident that there is no scheme that provides adequate security. There is also no scheme in the Table 4.1 with adequate security index.

The proposed authentication schemes in Table 4.1 have been evaluated against the security and privacy properties mentioned in Chapter 2 and listed as follows:

A1: Ensure user anonymity
A2: Resist insider attack
A3: Ensure efficient password update
A4: Ensure session key verification
A5: Ensure forward secrecy
A6: Resist denial of service attack
SI: Security index

Table 4.1: Comparison of one-factor authentication schemes

Scheme	A1	A2	A3	A4	A5	A6	SI
Lamport [6]	×	×	×	×	×	✓	1
Shimizu [94]	×	×	–	×	×	×	0
Harn [95]	×	×	✓	✓	✓	✓	4
Steiner [96]	×	×	✓	×	×	×	1
Bellovin et al. [97]	×	×	×	✓	×	×	1
Haller et al. [98]	×	✓	×	×	✓	✓	3
Gwoboa [99]	✓	×	✓	×	×	×	2

4.4 Conclusion

After the evaluation and analysis of one-factor authentication schemes, it is concluded that one-factor authentication schemes do not provide adequate security and also fail to ensure user privacy as well. Due to the insufficient security and privacy properties, the one-factor authentication schemes are strongly discouraged for e-Healthcare systems.

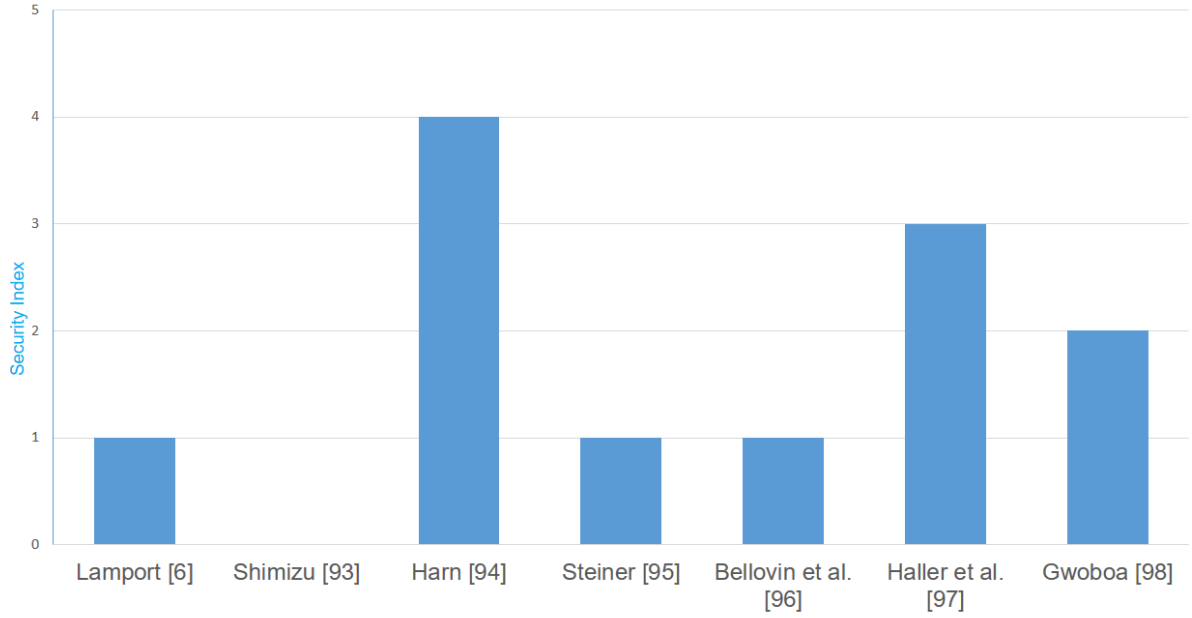

Figure 4.1: Comparison of one-factor authentication schemes

Chapter 5

TWO-FACTOR AUTHENTICATION SCHEMES

5.1 Introduction

Chapter 5 contains the evaluation of two-factor authentication schemes. In Section 5.2, two-factor authentication schemes have been evaluated. Pros and cons of authentication schemes have been described in detail and comparison of two-factor authentication schemes have been made on the basis of their security and privacy properties as well as on their computation cost. A tabular comparison have also been presented in Table 5.1 and 5.2 for better understanding of the reader. Later in the Section 6.3, a detailed analysis is given for the two-factor authentication schemes and based on the analysis a conclusion has also been drawn for the readers.

5.2 Two-Factor Authentication Schemes

The first ever two-factor authentication scheme was proposed by Hwang et al. [7] in 1990. In two-factor authentication schemes, a smart card is used as the second layer of security in addition to a password. Figure 5.1 explains the process of two-factor authentication. First, the user inserts his/her smart card into the smart card reader, the TMIS verifies the legitimacy of the smart card. After that, the TMIS asks for the username and password for the second layer of security, the user provides the requested credentials, the smart card processes them before sending them to TMIS, the TMIS checks the authenticity and approves or disapproves the access request. Some of the two-factor authentication schemes are discussed below:

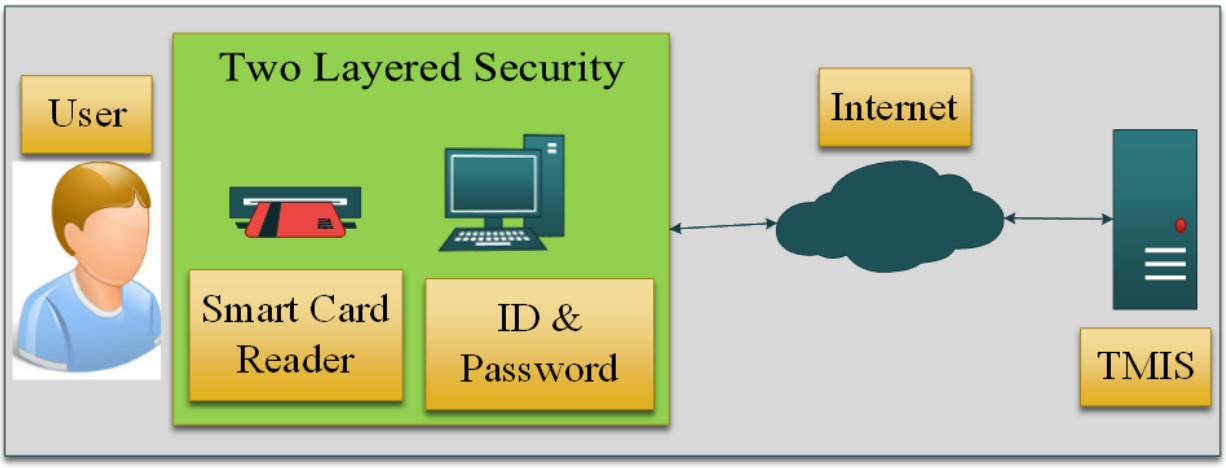

Figure 5.1: Two-factor authentication architecture

5.2.1 Hwang et al. scheme

The first ever smart card based two-factor authentication scheme was proposed by Hwang et al. [7] in 1990. It was a non-interactive password authentication scheme without the password tables. The scheme is based on Shamir's ID-based signature scheme [54] to solve the password storage problems and has equivalent security to that of Shamir's scheme. Hwang's [7] scheme does not contain any password table; the remote machine does not contain any secret for authentication phase; the scheme is non interactive; no one can masquerade as the legitimate user even after capturing the authentication messages; and it can verify login requests very easily and resist the replay attack.

5.2.2 Chang's scheme

One of the early two-factor authentication schemes was proposed by CC Chang [100] in 1991. In his scheme, he introduced the concept of a smart card where each user gets the smart card after successful registration and is essential for the login purpose. In the initial/registration phase of this scheme, the user registers with the remote system, which generates the password for the

user according to the presented identity. The password and the smart card containing the secret information are delivered to the user by a secure channel after successful registration. In the login phase, the user inserts the smart card into the smart card reader terminal and submits the ID and password. The remote system verifies the submitted ID and password by the user after validating the smart card, and on the basis of that it grants or rejects the access request. The scheme [100] solves the problem of password tables or verifier tables for each user at the remote server as it does not store the password at the server.

5.2.3 Das et al. scheme

One of the first dynamic ID-based remote user authentication scheme was proposed by Das et al. [23]. The proposed scheme gives an option to users to choose and update their password freely and does not store or retain any verifier table at the remote server. In 2009, Wang et al. [101] showed that Das et al's scheme is independent of a password. For authentication, an adversary requires only the smart card, and the scheme accepts all passwords because it does not verify the user password. Any password in the presence of a legitimate smart card will be accepted and the user will be granted access. The scheme had many advantages over the schemes [6, 15, 102, 103, 104, 105, 106, 107] presented in the last two decades. However, the scheme [23] does not ensure mutual authentication as the user cannot verify the remote server. Thus, the scheme fails to resist against the server impersonation attack.

5.2.4 Wang et al. scheme

To overcome the weaknesses presented in Das et al's scheme [23], Wang et al. [101] proposed their own scheme and stated that it is more secure, provides complete anonymity and more efficient than that is [23], as it solves the password independence issue presented in [23] and also

provides mutual authentication. Additionally, the security and secrecy of the password is strengthened, as the password is chosen by the remote system, which reduces the chances of user choosing a weak password. However, Khan et al. [108] proved that this scheme fails to ensure resistance against the insider attack, does not ensure user anonymity during authentication phase, has no revocation mechanism in case of a lost or stolen smart card, and does not provide freedom to the user in choosing a password. In the verification phase, the user's ID is transmitted in plain to the server through an insecure channel, which compromises the user anonymity.

5.2.5 Khan et al. scheme

Khan et al. [108] proposed an authentication protocol and stated that their protocol addresses all the weaknesses presented in [101] and offers more security features that were not present in [101]. The scheme in [108] provides an anonymous identity for the user at each login attempt to preserve user anonymity. The scheme binds the session key with timestamps to resist against replay attack. Chen et al. [109] and Jiang et al. [110] highlighted the weaknesses in [108] and proved that the scheme does not ensure resistance against the insider attacks, the secret key is shared among all insiders and hence fails to ensure user anonymity as an insider can obtain other users ID via a simple XOR operation. The scheme does not verify the correctness of the password at the smart card end and hence any password can be provided by the adversary in the password update phase. The scheme in [108] is vulnerable to identity guessing, as an adversary can guess the identity of the legitimate user via an offline exhaustive guessing attack. The scheme [108] also suffers from the tracking attack, as the different authenticated sessions of the user can be linked to a particular smart card.

5.2.6 Chen et al. scheme

Chen et al. [109] stated that their scheme addresses all the issues presented in [108]. The proposed scheme [109] hides the user's real identity by a random number in order to provide user anonymity. It provides mutual authentication by using the server's secret parameter, which can only be known to the user. The user sends the secret parameter to the server, which authenticates the user and the server sends the authenticated message to the user so that the user can also authenticate the server. The scheme also resists against impersonation attack, replay attack, man-in-the-middle attack, insider attack and also provides a revocation mechanism for stolen or lost smart cards. However, Jiang et al. [110] proved that the scheme does not ensure user anonymity, untraceability and also suffers from identity guessing attack.

5.2.7 Jiang et al. scheme

Jiang et al. [110] proposed an authentication scheme that allows the user to update their temporary identity after the successful login to preserve user privacy. The scheme uses cipher block chaining mode, in order to resist against insertion, deletion and modification attacks. However, Wu et al. [72] and Kumari et al. [111] exposed weaknesses in [110]. Wu et al. [72] proved that in the login phase of the scheme in [110], the user inserts the smart card in the terminal and inputs their ID and password for authentication purposes, but the smart card does not use the given ID. Instead, it uses the stored ID within the card, which makes the inserted user ID useless and enables an adversary to use the smart card without any knowledge of the legitimate user ID to access the remote server. Thus, the scheme fails to ensure resistance against the impersonation attack and the offline password guessing attack. Once the adversary successfully logins, he/she can get the next authentication message necessary for the next session login. The legitimate user will not

be able to login to a new session, as he/she does not own the authentication messages and will have to register again with the system. In the password change phase, the scheme [110] does not verify the old password before allowing the user to choose the new one, so the password change phase is insecure. Kumari et al. [111] proved that the scheme [110] is excellent in providing user anonymity and untraceability but overlooked some other security features and hence, fails to ensure resistance against the impersonation attack, guessing attack and DoS attack.

5.2.8 Wu et al. scheme

Wu et al. [72] proposed an authentication scheme that addresses issues presented in [110]. It uses a random number along with the password, in order to resist against the offline password guessing attack, it does not use any verifier table and the password is also one-way hash protected in the registration phase, in order to resist against the insider attack. The scheme [72] resists against DoS attack, replay attack and stolen verifier attack. He et al. [112] exposed the weaknesses in the scheme proposed in [72] and proved that it is vulnerable to impersonation attack as the user identity is independent of secret values in the login phase. In the first step of the registration phase, the legitimate user password is revealed to the server, which enables any insider privileged to have access to the server to steal the password and use it to access the other servers as a legitimate user. As users usually use the same password to access multiple servers, an administrator of one server can use the legitimate user's credentials to access the services offered by other servers.

5.2.9 He et al. scheme

He et al. [112] proposed an authentication scheme to address the weaknesses presented in [72]. The proposed scheme depends on the user identity, which is missing in the scheme in [72]. It does not reveal the user password to the server, instead its hash is presented to the server in

the registration phase, in order to resist against the insider attack. Due to the use of a random number along with the password, the chances of a successful offline password guessing attack is very limited. The scheme resists against replay attack as it checks the freshness of the received messages. However, Wei et al. [73] and Lee et al. [113] proved later that the scheme in [112] fails to ensure resistance against the offline password guessing attack, as the data in the smart card can be compromised. The scheme [112] also does not ensure mutual authentication as the user does not authenticate the remote server during the authentication process.

5.2.10 Wei et al. scheme

Wei et al. [73] proposed an authentication scheme and stated that it is more secure and efficient than the other proposed schemes. The scheme in [73] uses a random number along with the password during the hash calculation. The random number does not travel on the channel and also it is never stored in order to resist against the offline password guessing attack. The hash of the user password concatenated with the random number are sent to the server instead of the plain password during the registration phase, in order to resist against the insider attack. Using the remote system's secret key during the authentication phase makes the protocol resistant against the server impersonation attack, as no one can have the server's secret key except the server itself. However, Zhu et al. [114] showed that the scheme [73] does not solve the offline password guessing attack problem in case the smart card is stolen or lost. The random number concatenated with password is required for login purpose, as server matches the hash received during the registration phase, without the random number the user cannot compute the same hash again for the login purpose.

5.2.11 Lee et al. scheme

Lee et al. [113] proposed an authentication scheme to address the weaknesses presented in [73]. The proposed scheme provides mutual authentication, as both the user and the server authenticate each other during the authentication phase. The session key is protected by a one-way hash function during its transmission, so an adversary cannot derive it from the revealed messages. The user ID is protected by encrypting it with the one-way hash function during transmissions, in order to provide user anonymity. Das et al. [115] later proved that the scheme in [113] has weaknesses in the authentication phase, where a user mistakenly enters the wrong password and the server terminates the session instead of asking the correct password again and considers the user as a malicious one, and on the other hand the user does not know why his request is rejected and may consider the server as a cheater. In the password update phase, the server does not verify the correctness of the old password before accepting the new one from the user.

5.2.12 Xu et al. scheme

Xu et al. [116] proposed a two-factor authentication and key agreement scheme based on elliptical curve cryptography. The scheme preserves the user anonymity by ensuring the channel security during the submission of the user ID to the TMIS in the registration phase, and uses dynamic IDs during the authentication phase. It provides mutual authentication as the server can authenticate the user and vice versa. The scheme generates unique session keys, so the compromise of one session key does not impact the other sessions. The strength of the scheme lies on the fact that the ID of the user travels only on the secure channel, and hence it ensures resistance against the online and offline password guessing attacks, stolen smart card attack and the impersonation attack. However, Islam et al. [117] exposed weaknesses in [116] and proved that during the login

phase, the scheme [116] does not achieve a strong authentication. For example, when the user inserts his/her smart card into the smart card reader and inputs his/her ID and password, the smart card forwards the ID and password to the server without verifying it at its own end, so when a user enters the wrong credentials by mistake then the session is rejected by the server, which leads to an increase in computational and communication cost. The password change phase is independent of the user ID so anyone with the knowledge of only the password can change it without submitting the valid ID to TMIS. The scheme in [116] also does not verify the old password at the smart card level in the password update phase, and also vulnerable to replay attacks.The revocation mechanism in case of a lost or stolen smart card is not taken into consideration by the scheme.

5.2.13 Islam et al. scheme

Islam et al. [117] proposed their own scheme to address all the issues presented in [116]. In their scheme the user ID is dynamically changed using the timestamp for each session and also kept secret, in order to provide user anonymity. It uses a random number and TMIS's secret key along with an ID and password, in order to resist against the offline password guessing attack. The proposed scheme provides mutual authentication, where at first the TMIS validates the user and then the user validates the server on the basis of current timestamps. In the registration phase, the password and a randomly chosen random number is kept secret even from the TMIS, in order to resist against the insider attack. However, Chaudhry et al. [118] and Zhang et al. [119] exposed weaknesses in [117] and proved that the scheme does not resist against the server and user impersonation attack, as the adversary can extract the secret information from the smart card using power analysis.

5.2.14 Jiang et al. scheme

Jiang et al. [120] proposed an authentication scheme that encrypts the user ID with the server secret key to ensure user anonymity during the authentication phase. It provides mutual authentication, as the user and the server both authenticate each other before starting any kind of communication. Authentication messages in each session are unique so that the attacker cannot use them to track the user. In the registration phase, the hash of the password along with a random number are sent to the server, in order to resist against the insider attack. However, Mishra et al. [121] exposed weaknesses in [120] and proved that the scheme in [120] efficiently resists the impersonation attack, password guessing attack, privileged insider attack, stolen smart card attack and also ensures forward secrecy. Unfortunately, the scheme [120] does not verify the correctness of the user identity and password at the end-user during the password update phase. If a user mistakenly inputs wrong credentials during the password update phase, then the password is updated at the end-user and the session is rejected by the server. As a result, the user will face denial of service.

5.2.15 Zhang et al. scheme

Zhang et al. [119] proposed an authentication scheme to address the weaknesses presented in [117]. The proposed scheme [119] uses a secret value along with the user ID and does not reveal that to the server, in order to resist against the insider attack. Using the secret value along with the ID and password make the scheme resistant against the offline password guessing attack as in this case the user is required to guess the secret value in addition to the ID and password, which makes the attack infeasible. The strength of the scheme lies on the fact that it uses the secure channel while submitting the user ID to the TMIS in the registration phase, the password update phase, and in the revocation phase. Due to this, the scheme provides user anonymity and an efficient

password update phase, and also resists against the online and offline password guessing attacks. However, Tu et al. [122] proved that the scheme fails to resist against the impersonation attack.

5.2.16 Tu et al. scheme

Tu et al. [122] proposed a scheme that is 75% replica of Zhang et al. [119] scheme. Their cryptanalysis shows that the scheme in [119] only fails to resist against the impersonation attack. So, they proposed an improvement only for this issue as the scheme in [119] resists against all other known attacks. In their proposed scheme, the user uses a secret value to generate the legal messages during the authentication phase, in order to resist against the user impersonation attack. However, Chaudhry et al. [123] and Farash et al. [124] exposed weaknesses in this scheme and proved that the scheme in [122] is vulnerable to impersonation attack, user anonymity, replay and denial of service attack. An adversary can impersonate as a legitimate user without knowing the private/secret key. This attack can be successfully performed by an adversary by intercepting the authentication messages. Tu et al. [122] did not discuss the privacy and anonymity issue in their scheme. As the login request does not contain any timestamps, an adversary can replay the intercepted login messages later on. By sending login requests in bulk, an adversary can launch a denial of service attacks as there are no timestamps.

5.2.17 Farash et al. scheme

Farash et al. [124] proposed an authentication scheme to address the weaknesses presented in [122]. The scheme uses a secret value to compute the authentication messages in contrast to the scheme in [122], in order to resist against the impersonation attack and offline password guessing attack . However, Kumari et al. [125] proved that the scheme does not resist against the impersonation attack, which is performed by an adversary intercepting the login requests and

computing username to get secret parameters and impersonate as the legitimate user. It is also vulnerable to the password guessing attack in case of stolen or lost smart card, anonymity and session specific temporary information attack.

5.2.18 Wen et al. scheme

Wen et al. [126] proposed an authentication scheme that hides the user identity in authentication messages, in order to provide the user privacy. As the ID is hidden, the adversary needs to guess the ID of the user as well as the password, which makes the attack infeasible. It resists against the replay attack, as each message contains the tiestamps and a random nonce. However, many researchers found several vulnerabilities in this scheme. So, Wen proposed another scheme [127] to address the weaknesses found in the previous scheme [126]. However, Xie et al. [128] proved that the scheme in [127] does not provide user anonymity and perfect forward secrecy and also vulnerable to off-line password guessing attack.

5.3 Analysis - Comparison of Two-Factor Authentication Schemes

Early smart card based schemes were based on the assumption that the information stored in the smart card cannot be extracted. The strength of those schemes lies on this assumption. So, Hwang and Chang [7, 100] did not even bother to encrypt the information stored on the smart card. The user identity and password are stored in the plain, inside the memory of the card. In 1999, Paul C Kocher proposed a method [129] for the extraction of information stored in the smart card. Later, many researchers proposed different models for extracting the information from the smart card [130, 42, 131, 132, 133, 134, 135]. After Kocher, researchers started using one way hash functions to encrypt the information stored on the smart card.

As the early schemes did not consider TMIS as the remote system, these schemes did not dis-

cuss the anonymity, privacy and untraceability issues. In our study, we left those schemes and mentioned only few of them for the sake of understanding. The biggest challenge in two-factor authentication schemes is to resist against stolen or lost smart card attacks, as the adversary in this case could have physical access to the card and can extract the stored information.

A new factor of security is needed to strengthen the authentication schemes that cannot be easily guessed, stolen or lost. Comparison of the security and privacy properties provided by the two-factor authentication schemes is presented in Table 5.1 and in Figure 5.2 while the computation cost comparison is given in Table 5.2 and in Figure 5.3. The security index in Table 5.1 refers to the number of security and privacy properties ensured by the scheme. From Table 5.1, it is evident that there is no scheme that provides complete security. There are only few schemes that have a higher security index with a high user efficiency.

The proposed authentication schemes in Table 5.1 have been evaluated against the security and privacy properties mentioned in Chapter 2, Section 2.3 and listed as follows:

A1: Ensure user anonymity

A2: Resist insider attack

A3: Ensure efficient password update

A4: Ensure session key verification

A5: Ensure forward secrecy

A6: Resist denial of service attack

A7: Resist off-line password guessing attack

A8: Resist stolen smart card attack

A9: Resist user impersonation attack

A10: Resist stolen verifier attack

A11: Resist replay attack

SI: Security index

Similarly, user and server efficiency have been divided in three categories. The proposed schemes in Table 5.2 have been evaluated against the designed performance metrics mentioned in Chapter 3 and listed as followed:

Efficiency : The total number of operations performed by the user and the server

High efficiency : Total number of operations ≤ 05

Medium efficiency : $08 \geq$Total number of operations ≥ 06

Low efficiency : Total number of operations ≥ 08

There is a reason that Table 5.2 highlights the user and server efficiency in separate columns, in the login phase, the user inserts his/her smart card into the smart card reader, once the smart card is authenticated by the TMIS, the user is asked to provide his/her username along with the password, and then the algorithm in the smart card computes operations as designed and forwards them to the TMIS for authentication. In the authentication phase, TMIS verifies the forwarded information and approves or disapproves the access request.

The user efficiency is measured by the computations performed by the smart card at the end-user, while server efficiency is measured by the computations performed by the TMIS at the remote server. It is also worth mentioning that at any given time TMIS authenticates several users at a time while a user can only send one access request at a time. At peak times the user may face denial of service as TMIS may not process new requests due to exhaustion, therefore user and server efficiency should be discussed separately.

After the evaluation and analysis of two-factor authentication schemes, it is concluded that there are only few schemes in Table 5.2, which have high user efficiency and also ensure seven or more security properties. It can also be noted that these schemes are either not widely scrutinized by the researchers or they do not verify the user legitimacy at the end-user, which saves lot of operations

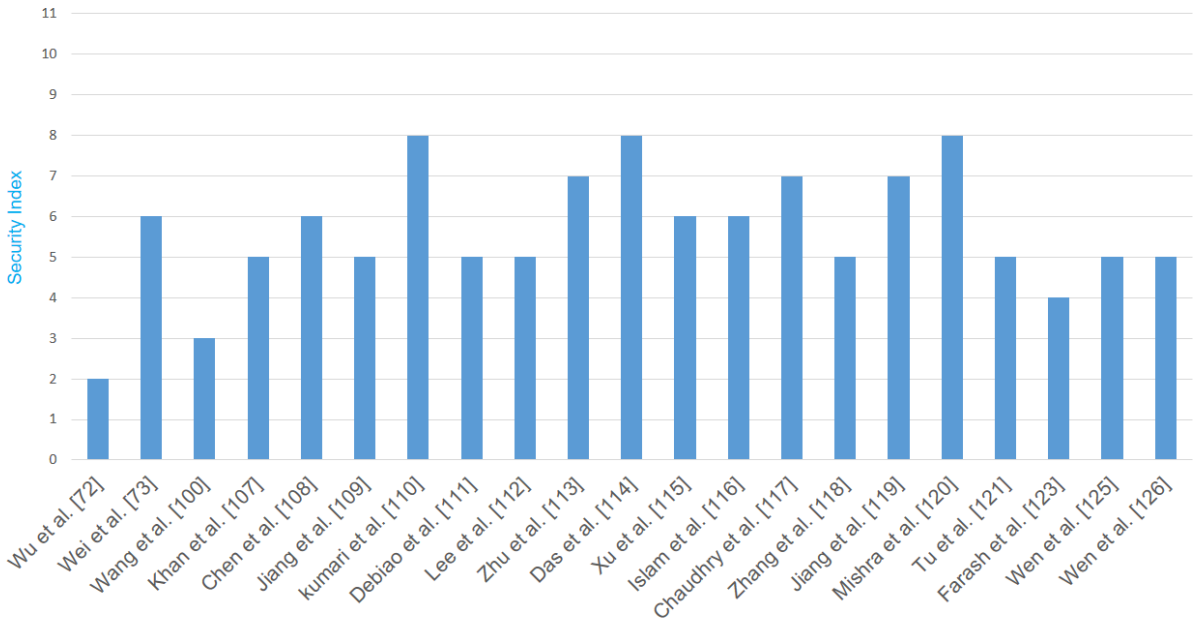

Figure 5.2: Security performance comparison of two-factor authentication schemes

and therefore results in high user efficiency, e.g, the scheme in [111] has a moderate user efficiency and ensures eight security properties but it is not widely crypt-analyzed, and similarly the scheme in [116] has very high user efficiency and also ensures six security properties but the scheme does not verify the user legitimacy at the end-user.

5.4 Conclusion

After the evaluation and analysis of two-factor authentication schemes, it is concluded that current two-factor authentication schemes tend to provide sufficient security and privacy properties at the cost of computation cost, communication cost and user easiness, however, the current two-factor authentication schemes fail to ensure complete security and privacy properties mentioned in performance metrics. The two-factor authentication schemes can be improved to ensure security and privacy properties. The well designed two-factor authentication schemes which can also satisfy the performance metrics may be used for user authentication in e-Healthcare system.

Table 5.1: Security and privacy properties of two-factor authentication schemes

Scheme	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	SI
Wu et al. [72]	–	✓	×	×	–	×	×	×	✓	×	×	2
Wei et al. [73]	×	✓	×	✓	×	×	×	✓	✓	✓	✓	6
Wang et al. [101]	×	×	×	×	–	–	×	✓	✓	–	✓	3
Khan et al. [108]	×	×	×	✓	–	–	×	✓	✓	✓	✓	5
Chen et al. [109]	×	✓	✓	×	×	✓	×	✓	×	✓	✓	6
Jiang et al. [110]	✓	✓	✓	–	×	×	×	×	×	✓	✓	5
kumari et al. [111]	✓	✓	✓	–	×	✓	✓	×	✓	✓	✓	8
Debiao et al. [112]	×	✓	✓	✓	–	×	×	×	✓	×	✓	5
Lee et al. [113]	–	×	×	✓	–	×	✓	✓	✓	✓	×	5
Zhu et al. [114]	×	✓	×	–	✓	×	✓	✓	✓	✓	✓	7
Das et al. [115]	×	✓	✓	✓	–	–	✓	✓	✓	✓	✓	8
Xu et al. [116]	✓	✓	×	–	✓	×	✓	×	✓	✓	×	6
Islam et al. [117]	✓	✓	✓	–	✓	–	✓	×	×	×	✓	6
Chaudhry et al. [118]	✓	✓	✓	–	✓	–	✓	–	–	✓	✓	7
Zhang et al. [119]	×	✓		×	✓	×	✓	✓	×	✓	×	5
Jiang et al. [120]	✓	–	×	×	✓	×	✓	✓	✓	✓	✓	7
Mishra et al. [121]	✓	✓	✓	✓	✓	✓	×	×	×	✓	✓	8
Tu et al. [122]	×	✓		×	✓	×	✓	✓	×	✓	×	5
Farash et al. [124]	×	✓	✓	×	–	✓	×	×	×	×	✓	4
Wen et al. [126]	×	✓	✓	–	×	✓	×	×	✓	–	✓	5
Wen et al. [127]	×	✓	–	–	×	✓	×	✓	✓	–	✓	5

Table 5.2: Computation cost of two-factor authentication schemes

Scheme	UC	UE	SC	SE
Wu et al. [72]	$6T_h + 2T_s$	M	$5T_h + 2T_s$	M
Wei et al. [73]	$5T_h + 1T_{pm} + 1T_{me}$	M	$5T_h + 1T_{pm} + 1T_{me}$	M
Wang et al. [101]	$2T_h$	H	$4T_h$	H
Khan et al. [108]	$3T_h$	H	$5T_h$	H
Chen et al. [109]	$5T_h$	H	$5T_h$	H
Jiang et al. [110]	$3T_h + 1T_s$	H	$3T_h + 3T_s$	M
kumari et al. [111]	$5T_h + T_s$	M	$3T_h + T_s$	H
Debiao et al. [112]	$5T_h + 1T_{me}$	M	$4T_h$ + $1T_{pa} + 1T_{minv}$	M
Lee et al. [113]	$7T_h + 2T_{ch}$	L	$8T_h + 2T_{ch}$	L
Zhu et al. [114]	$4T_h + 1T_{me}$	H	$4T_h + 1T_{me}$	H
Das et al. [115]	$7T_h + 1T_{me}$	M	$7T_h + 1T_{me}$	M
Xu et al. [116]	$2T_h + 2T_{pm}$	H	$9T_h + 4T_{pm}$	L
Islam et al. [117]	$6T_h + 2T_{pm}$	M	$3T_h + T_{pm}$	H
Zhang et al. [119]	$6T_h + 4T_{pm} + 1T_{pa}$	L	$5T_h + 4T_{pm} + 1T_{pa} + 1T_{minv}$	L
Jiang et al. [120]	$2T_h + T_s + 3T_{ch}$	M	$1T_h + 2T_s + 3T_{ch}$	M
Mishra et al. [121]	$5T_h + 1T_{ch}$	M	$5T_h + 1T_{ch}$	M
Tu et al. [122]	$5T_h + 4T_{pm} + 1T_{pa}$	L	$5T_h + 3T_{pm}$	L
Chaudhry et al. [123]	$5T_h + 3T_{pm}$	M	$3T_h + 1T_{pm}$	H
Farash et al. [124]	$5T_h + 4T_{pm} + 1T_{pa}$	L	$5T_h + 3T_{pm}$	M
kumari et al. [125]	$5T_h + 4T_{pm} + 1T_{pa}$	L	$6T_h + 2T_{pm}$	M
Wen et al. [126]	$3T_h + 2T_s + 4T_{me} + 1T_{pm}$	L	$2T_h + 2T_s + 4T_{me} + 1T_f$	L

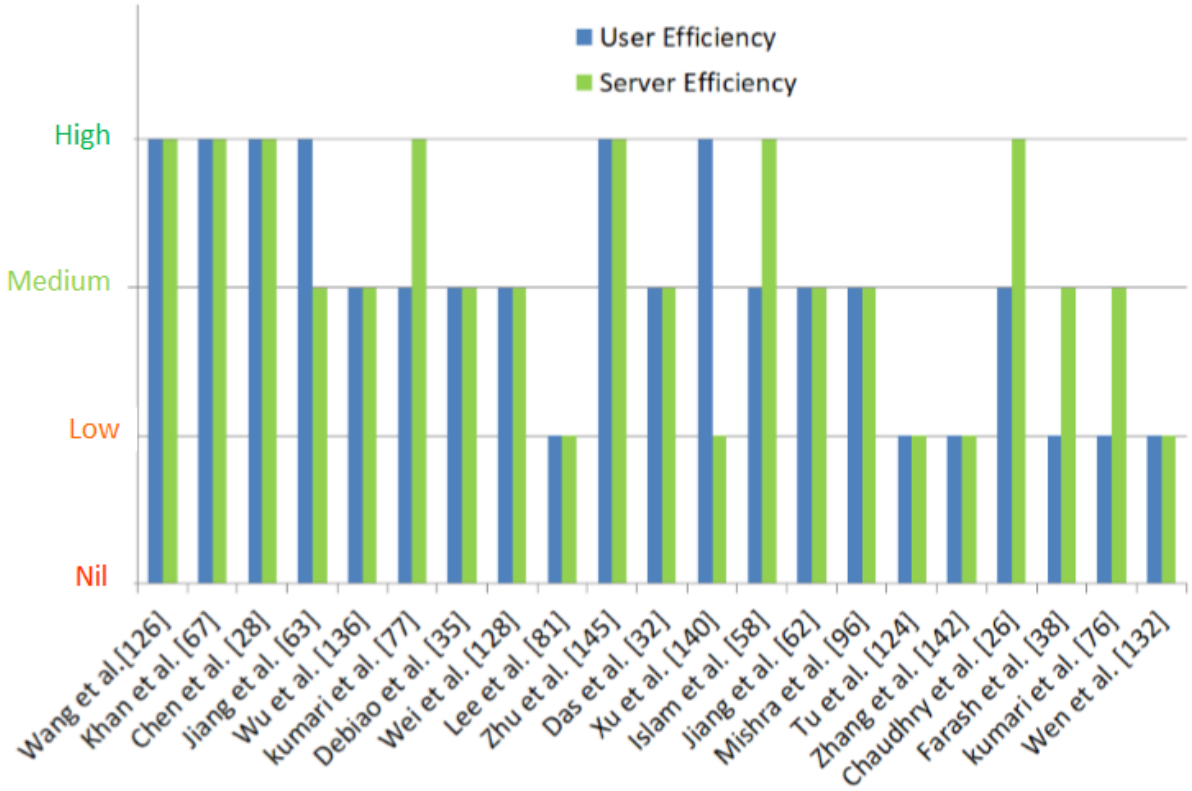

Figure 5.3: Computation performance comparison of two-factor authentication schemes

Chapter 6

THREE-FACTOR AUTHENTICATION SCHEMES

6.1 Introduction

Chapter 6 contains the evaluation of three-factor authentication schemes. In Section 6.2, three-factor authentication schemes have been evaluated. Pros and cons of authentication schemes have been described in detail and comparison of three-factor authentication schemes have been made on the basis of their security and privacy properties as well as on the basis of their computation cost. A tabular comparison have also been presented for better understanding. Later in the Section 6.3, a detailed analysis is given for the three-factor authentication schemes. The last Section **??** contains the conclusion of the chapter based on the evaluated schemes.

6.2 Three-Factor Authentication Schemes

In three-factor authentication schemes, the user's biometric information is used as the third layer of security in addition to a smart card and password. In this method, the user proves his/her identity by providing his/her biometric information before proving the authenticity of the smart card and secret password. Figure 6.1 explains the process of three-factor authentication, and some of the three-factor authentication schemes are discussed below:

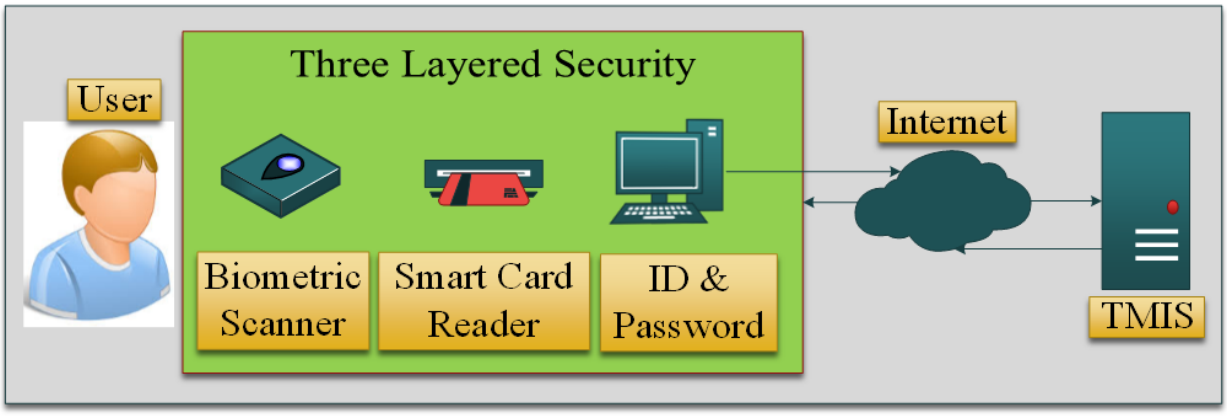

Figure 6.1: Three-factor authentication architecture

6.2.1 Chang et al. scheme

Chang et al. [136] proposed one of the first three-factor authentication schemes for TMIS and stated that the existing two-factor authentication schemes do not protect user privacy as the user can be traced using the data they transmit. In addition, the verification tokens used by these schemes to authenticate the user or server are not unique and only the password and the smart card/RFID tag are unique. These verification tokens are easy to copy and one legitimate user can impersonate as another legitimate user. The scheme in [136] depends on the biometric information of the user as the third layer of the security. The scheme resists to stolen smart card attack, as the smart card is not enough to access the TMIS, and the adversary requires the legitimate user's biometric information as well. The scheme uses a secret random value along with the user ID and encrypts them using a one-way hash function before transmitting them on the channel, in order to resist against the impersonation attack. It uses dynamic IDs for each session, in order to provide user anonymity. However, Das et al. [137] proved that in the login phase, the smart card does not verify the user password, and hence the rejection is issued by the server, which increases the computational and communication cost. As the password is not verified at the smart card level, so if the user inputs a wrong password by mistake, the smart card will update the new password but

as the old password is not correct, the session will be rejected by the server. Consequently, two different passwords will be stored at the end-user and the server, and hence the user will not be able to login to the TMIS ever again. The only solution to resolve this problem is to renew the user registration with TMIS and get another smart card. In their proposed scheme, the password of the user is revealed to the server considering it trustworthy, so an insider having access to the server can use the password and impersonate as a legal user. Generally, users use the same password for multiple services, hence, the adversary can impersonate as a legitimate user to access all the services, for which the user has the same password. As a result, the scheme fails to resist against privileged insider attack. The validity of the login messages relies only on the format of the user identity and corresponding random number given to the user by the server. Since the scheme fails to verify the validity of the authentication messages, this provides an opportunity to any adversary to tamper the message. As a result, it leads the user to believe that the server is a cheater, which is actually not true.

6.2.2 Das et al. scheme

Das et al. [137] exposed weaknesses in [136] and proposed improvements. The improved scheme [137] always verifies the user biometric information, the corresponding smart card, ID and password at the end-user before forwarding them to the server during the login phase. It gives freedom to the user to update their password even in server's absence during the password update phase, and the scheme does not reveal the user biometric information and password to the server in order to resist against any insider attack. Das et al. [137] claimed that their scheme addresses all the vulnerabilities found in [136] and provides better security against active and passive attacks. However, Kim and Lee [138], and also Wen et al. [139] proved that the scheme is vulnerable to user impersonation attack, offline password guessing attack and also does not ensure forward se-

crecy and user anonymity. Kim and Lee [138] proved that if an attacker obtains the master secret key from the compromised server and eavesdrops an authentication messages then the attacker can use the master secret key to reveal the user's identity by plotting the dictionary attack and derive previous session keys.

6.2.3 Xie et al. scheme

Xie et al. [128] proposed a scheme to address the weaknesses in [127]. The proposed scheme does not store the user identity at the smart card, which makes the stolen smart card attack harder, as the adversary also requires the ID of the user in addition to the password and biometric information, in order to access the TMIS. The scheme does not transmit the user ID in plain on the communication channel and also uses a secret value along with the user ID, in order to resist against the impersonation attack. However, Xu et al. [140] proved that the scheme is vulnerable against de-synchronization attack, and also puts too much storage burden on the server. As Xie et al. [128] do not use a bio-hash function to deal with the user biometric information, it is obvious that the biometric information that travels on the communication channel during the login and authentication phase would be different from the stored information at the server, and hence, the login request will be denied by the TMIS. In the login phase, the user's chosen random identity is only updated when the server receives all the authentication messages in sequence, and if an attacker blocks or delays one of the intermediate messages then the update will only happen at the user side, and the session will be rejected by the server as it did not receive all the messages or not in a correct sequence. Xie et al. [128] use a verifier table, which consumes a lot of storage space and puts an extra burden on the server as compared to other schemes.

6.2.4 Xu et al. scheme

Xu et al. [140] proposed an authentication scheme to address the weaknesses of [128]. In the login phase of the scheme, the user only submits a random identity to the server, so that the eavesdropper and the insider cannot learn the real identity of the user, in order to resist against the insider attack and impersonation attack. The scheme uses a random number along with the password in the login and authentication phases in order to resist against the insider attack, offline password guessing attack, user impersonation attack, server spoofing attack and replay attack, as the adversary also needs to guess the random number in addition to the password and ID to make these attacks successful. However, Amin et al. [141] proved that the scheme in [140] has a design flaw, in the password update phase as it asks for the old password before accepting the new one but it does not verify the old password. This is disastrous if the smart card is stolen, because the adversary can change the password without the knowledge of the old password, as the scheme does not verify the old password. It also fails to achieve strong authentication in the authentication phase, fails to provide revocation mechanism for stolen or lost smart cards, and fails to resist against the strong replay attack.

6.2.5 Awasthi et al. scheme

Awasthi et al. [142] proposed an authentication scheme that focuses more on the efficiency to make it lighter and faster. The scheme in [142] uses a non invertible chaotic hash function in order to resist against the guessing attack. It uses an encrypted password with an appropriate nonce in the registration phase to hide the user identity and the corresponding password from the server, in order to resist against the insider attack. However, Tan et al. [143] exposed weaknesses in [142] and proved that the scheme fails to resist against the reflection attack, and also fails to

ensure user anonymity and three-factor authentication. Suppose that, an adversary is monitoring the channel and intercepts the response messages during the authentication phase, and then it uses these authentication messages and sends a login request to the server immediately. The server checks the legitimacy of the requests by verifying the format of the request messages, including the identity and the timestamps. In the given scenario, the format of the authentication messages is correct, the timestamps holds the current time when the remote system receives the request. So, the requirements for the authentication are met and the server believes that the login request is from the registered user and hence, the server sends a response message to the adversary and grants access to the remote server. In the scheme the user identity is sent in plain text over the network during the login phase, which compromises the user anonymity.

6.2.6 Tan et al. scheme

Tan et al. [143] proposed an authentication scheme to address the weaknesses presented in [142]. In the scheme [143], the user identity, password, and biometric information are verified at the end-user, and due to the use of a collision resistant one-way hash function during the authentication phase, the user ID, password and biometric information are hidden from the server and the eavesdropper, and only the user knows the correct identity, password and biometric information, in order to protect the scheme against the insider and the DoS attacks.

In the authentication phase, the server signs the reply messages with its private key, so that the user can also authenticate the server. In the password update phase, the user identity, password, and biometric information are verified first before updating them at the end-user side. In the scheme, the update can also take place without the server participation. The user sends an encrypted password to the remote server in the registration phase in order to resist against the insider attack. Arshad et al. [144] and Yan et al. [145] proved that the scheme in [143] has several security

weaknesses. As the TMIS fails to ensure the freshness of the messages, replay attack is possible. Due to the avalanche effect of the hash functions, the biometric information of the same user may vary each time and the server will not be able to authenticate the user in scheme [143], and hence the registered user may not be able to access the server and face a denial of service.

6.2.7 Arshad et al. scheme

Arshad et al. [144] proposed an authentication scheme to address all the weaknesses presented in [143] . The scheme proposed in [144] uses timestamps and two fresh random numbers in order to resist against replay attack, it uses the symmetric parametric function to verify the biometric information, and in order to reduce the computational complexity it uses two 160-bit modular multiplications and one 160-bit modular inversion. However, Lu et al. [146] proved that the scheme fails to resist against offline password guessing attack and once successful, an adversary can impersonate as a legitimate user of the TMIS.

The attack's success is based on the assumption that the adversary is completely monitoring the communication channel, and can eavesdrop, delete, insert or modify any message transmitted using the public channel. The password and identity have low entropy, which enhances the chances of successful offline attack, and if adversary succeeds, he/she can impersonate as a legitimate user.

6.2.8 Lu et al. scheme

Lu et al. [146] proposed a scheme to address the weaknesses presented in [144]. The scheme proposed in [146] conceals user's identity by a one-way hash function in transmitting messages, in order to ensure user anonymity during the login and authentication phase. The scheme uses the server's private key and user's biometric information in login messages, which makes the offline password guessing attack very hard because only the user and the server knows the biometric

information and the private key respectively. Chaudhry et al. [147] exposed the weaknesses of [146] and proved that the scheme does not ensure anonymity, and is vulnerable to the user and the server impersonation attack and does not provide user untraceability, when the adversary registers itself with the TMIS and acts as a dishonest user. A dishonest user D can easily break other users anonymity, as D registers with the TMIS system, gets his/her smart card containing the secret information and extracts them by means of power analysis. When an honest user pledges the authentication requests, D captures them and extracts user's ID by using the extracted information from his/her own smart card. Hence, D can successfully compromise the user's anonymity.

6.2.9 Chaudhry et al. scheme

Chaudhry et al. [147] proposed an authentication scheme to address the weaknesses in [146]. In the proposed scheme, in order to provide mutual authentication the server authenticates the user after verifying his/her smart card, password, and biometric information, and the user authenticates the server after verifying the messages that they are signed by the server by its private key. In the login phase, the user sends pseudo identity instead of the real one, in order to ensure user anonymity. To impersonate as the user, the adversary needs to generate the valid messages that cannot happen without the valid ID, password and biometric information of the legitimate user, and to impersonate as the TMIS, the adversary needs to generate the valid response messages that cannot be generated without the TMIS's secret key. In the registration phase, the password and biometric information are not revealed to the TMIS, and the TMIS also does not store any verifier table, in order to resist against the insider attack.

6.2.10 Yan et al. scheme

Yan et al. [145] proposed their scheme that uses a predetermined threshold for biometric verification in order to resist against the Denial-of-Service attack. In the registration phase, the user sends an encrypted password to the server, in order to resist against the privileged insider attack. The scheme does not use any verifier table, therefore it can resist against the stolen verifier attack. In the scheme, the server uses its private key to verify the user password, which makes the offline password guessing attack very hard, as the adversary cannot verify the correctness of the guessed password without the server secret key. However, Mishra et al. [148] exposed weaknesses in [145] and proved that the scheme fails to resist against the offline password guessing attack, it does not protect the user identity, and is vulnerable to the fake password change attack and the DoS attack. In the scheme [145], the user's real identity associates with the login messages, which reveals the sender information to any eavesdropper who listens to the channel. Hence, it does not protect user anonymity, the adversary can also guess the legitimate user's password with the help of the information extracted from the smart card and captured authentication messages. In the login phase, the identity and password are not verified at the end-user, therefore in the password update phase, if the user by mistake enters the wrong ID or password, the change will only take place at the end-user, and the session will be rejected by the server and the user will face denial of service every time he/she tries to login to access the server.

6.2.11 Mishra et al. scheme

Mishra et al. [148] proposed their own scheme to address all the weaknesses presented in [145]. In the login phase, the scheme [148] uses the user password along with biometric information to generate valid login messages, in order to resist against the stolen smart card attack and online

password guessing attack,as the adversary cannot generate valid login messages without the user password and biometric information, and guessing both of these information at the same time is infeasible. In login messages, the user's dynamic identity is used instead of the real one to ensure the user anonymity. However, Amin et al. [141] exposed weaknesses in [148] and proved that the scheme fails to ensure resistance against the offline password guessing attack and user impersonation attack. In the scheme in [148], an adversary can impersonate as a legitimate user by intercepting the authentication messages between the server and the legitimate user and later replaying them. The adversary can also impersonate as a valid user of the TMIS after getting the legitimate user's smart card by some means and replacing the server's secret key inside the smart card, as the smart card also contains the user password. As the adversary only changes the server secret key, the user password and user identity remains unchanged, and the format of the secret key is also valid, thus the adversary can access the remote server as a legitimate user.

6.2.12 Giri et al. scheme

Giri et al. [149] showed weaknesses in the scheme in [150] and proved that the scheme fails to ensure resistance against the offline password guessing attack and does not provide any revocation mechanism. An adversary can modify the intercepted authentication messages because of their low entropy. Giri et al. proposed their scheme [149] to address all the weaknesses presented in [150]. The proposed scheme is based on the RSA to make it efficient and practical. The scheme works on the assumption that the adversary cannot extract any secret information from the smart card and captured authentication messages, which is obviously not a true assumption as information stored in the smart card can be extracted using different ways [42, 130, 131, 132, 133, 134, 135].

6.2.13 Amin et al. scheme

Amin et al. [14] exposed a weakness in the scheme in [150] and proved that it suffers from offline password guessing attack, user anonymity and privileged insider attack. In [150], the server can trace the user, so the adversary can also trace the user by intercepting the login messages during the authentication phase, which compromises the user anonymity. Most users use the same password for multiple services, and if the adversary gets the user password he/she can access all the services, for which the user has the same password. An insider who can somehow get access to the user smart card and extract the password using offline password guessing attack, can use that password to access the other services subscribed by the user with the same password.

Amin et al. [151] also presented a novel idea recently, whereas all the present authentication schemes address the authentication issue between two parties, i.e., the user and the TMIS. They proposed an architecture of multiple authentication servers. In this architecture, the end-users can directly communicate with each other, e.g., a patient can directly communicate with the doctor or vice versa. Amin et al. [152] also proposed a new architecture for authentication schemes, in which three parties participate simultaneously for authentication.

6.3 Analysis - Comparison of Three-Factor Authentication Schemes

The comparison of security and privacy properties and computation costs among three-factor authentication schemes is given in Table 6.1 and in Table 6.2 respectively. The comparison of security and privacy properties and computation costs among three-factor authentication schemes in graphical form is given in Figure 6.2 and in Figure 6.3 respectively. Table 6.1 is very much similar to Table 5.1, as there is not a single scheme that ensures all the security and privacy properties. It can also be observed that the three-factor authentication schemes provide equivalent

security to two-factor authentication schemes at the cost of more computations. There are only three schemes [148, 141, 149] in Table 6.2 that have high user efficiency but among them the schemes in [148, 149] have a very low security index.

The security index in Table 6.1 refers to the number of security and privacy properties ensured by the scheme. From Table 6.1, it is evident that there is no scheme that provides complete security. There are only few schemes that have a higher security index with a high user efficiency.

The proposed authentication schemes in Table 6.1 have been evaluated against the security and privacy properties mentioned in Chapter 2, Section 2.3 and listed as follows:

A1: Ensure user anonymity

A2: Resist insider attack

A3: Ensure efficient password update

A4: Ensure session key verification

A5: Ensure forward secrecy

A6: Resist denial of service attack

A7: Resist off-line password guessing attack

A8: Resist stolen smart card attack

A9: Resist user impersonation attack

A10: Resist stolen verifier attack

A11: Resist replay attack

SI: Security index

The only scheme in Table 6.2 that has high user efficiency and also have high security index is the one in [141] but it is due to the fact that it has not been so far crypt-analyzed by any researcher and therefore it has a high security index. Most of the schemes in Table 6.2 have medium or low user efficiency and this is due to the added computations of bio-hashing.

Similarly, user and server efficiency have been divided in three categories. The proposed schemes in Table 6.2 have been evaluated against the designed performance metrics mentioned in Chapter 3 and listed as followed:

Efficiency : The total number of operations performed by the user and the server

High efficiency : Total number of operations ≤ 05

Medium efficiency : $08 \geq$Total number of operations ≥ 06

Low efficiency : Total number of operations ≥ 08

There is a reason that Table 6.2 highlights the user and server efficiency in separate columns, in the login phase, the user inserts his/her smart card into the smart card reader, once the smart card is authenticated by the TMIS, the user is asked to provide his/her username along with the password, and then the algorithm in the smart card computes operations as designed and forwards them to the TMIS for authentication. In the authentication phase, TMIS verifies the forwarded information and approves or disapproves the access request. The user efficiency is measured by the computations performed by the smart card at the end-user, while server efficiency is measured by the computations performed by the TMIS at the remote server. It is also worth mentioning that at any given time TMIS authenticates several users at a time while a user can only send one access request at a time. At peak times the user may face denial of service as TMIS may not process new requests due to exhaustion, therefore user and server efficiency should be discussed separately.

6.4 Conclusion

After the evaluation and analysis of three-factor authentication schemes, it is concluded that current three-factor authentication schemes tend to provide sufficient security and privacy properties at the cost of computation cost, communication cost and user easiness. The current three-factor authentication schemes fail to ensure complete security and privacy properties mentioned in per-

Table 6.1: Security and privacy properties of three-factor authentication schemes

Scheme	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	SI
Amin et al. [14]	✓	✓	✓	✓	–	–	✓	✓	✓	–	✓	8
Xie et al. [128]	✓	✓	✓	–	✓	×	✓	✓	✓	–	✓	8
Chang et al. [136]	✓	×	×	×	×	✓	✓	×	✓	×	✓	5
Das et al. [137]	✓	✓	✓	–	×	×	×	×	✓	✓	✓	6
Wen et al. [139]	✓	–	✓	✓	–	✓	✓	✓	✓	–	✓	8
Xu et al. [140]	✓	✓	×	×	–	×	✓	×	✓	–	×	4
Amin et al. [141]	✓	✓	✓	✓	–	–	✓	✓	–	–	✓	7
Awasthi et al. [142]	×	✓	✓	×	✓	✓	✓	✓	×	–	✓	7
Tan et al. [143]	✓	✓	×	–	✓	×	✓	✓	✓	–	×	6
Arshad et al. [144]	×	✓	✓	✓	✓	×	✓	✓	×	×	×	6
Yan et al. [145]	×	✓	×	×	–	✓	×	✓	✓	×	✓	5
Lu et al. [146]	×	✓	✓	–	✓	✓	✓	✓	×	×	✓	7
Mishara et al. [148]	×	✓	✓	–	–	✓	✓	×	×	–	×	4
Giri et al. [149]	×	✓	✓	×	–	–	×	×	✓	×	✓	4
Khan et al. [150]	✓	✓	×	–	✓	×	×	✓	✓	–	–	5

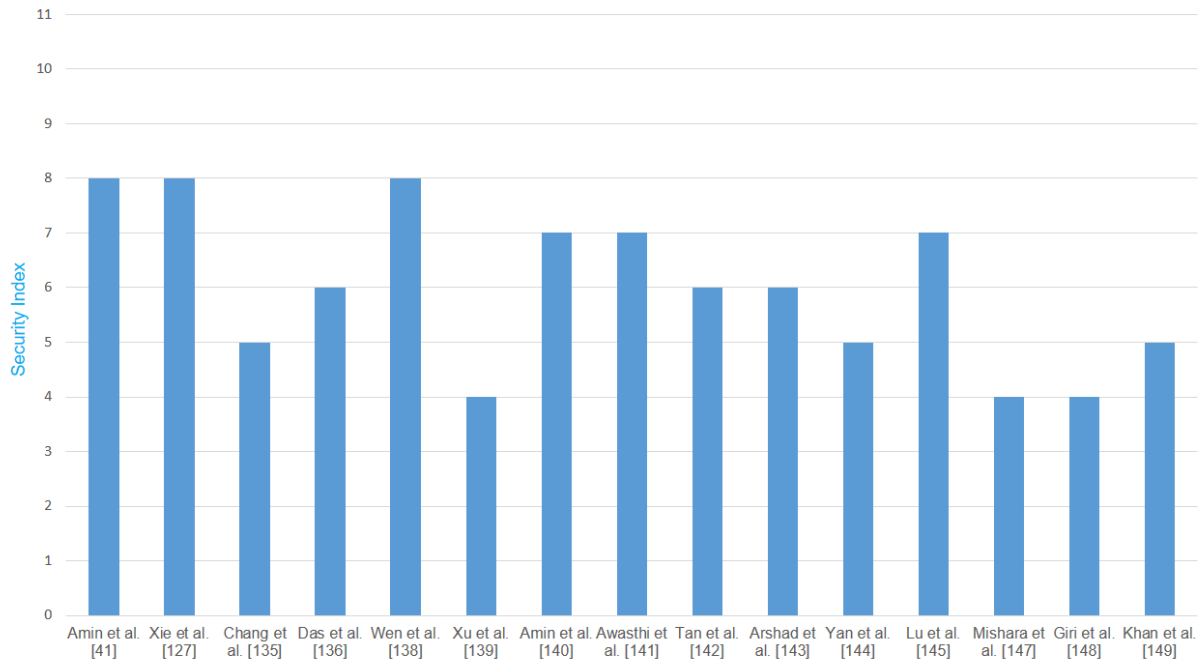

Figure 6.2: Security performance comparison of three-factor authentication schemes

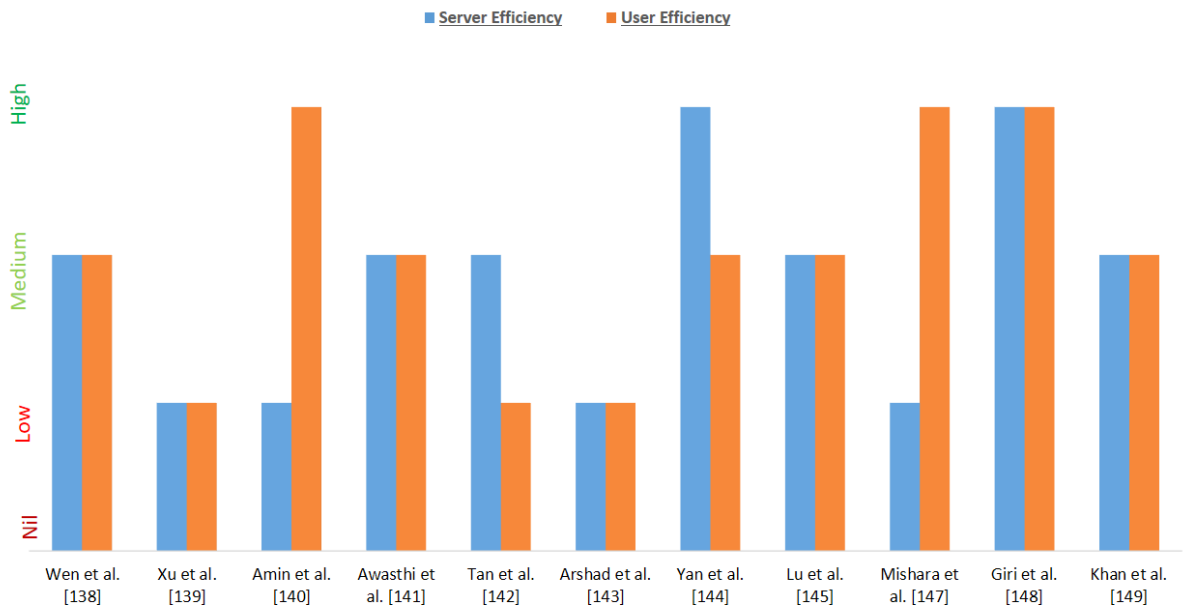

Figure 6.3: Computation performance comparison of three-factor authentication schemes

Table 6.2: Computation cost of three-factor authentication schemes

Scheme	UC	UE	SC	SE
Amin et al. [14]	$5T_h + 1T_{me}$	M	$8T_h + 1T_{me}$	L
Xie et al. [128]	$7T_h + 2T_{pm} + 1T_s$	L	$6T_h + 2T_s + 2T_{pm}$	L
Chang et al. [136]	$5T_h + T_H$	M	$4T_h$	H
Das et al. [137]	$9Th + 1TH$	L	$7T_h$	M
Wen at el. [139]	$7T_h + 1T_H$	M	$6T_h + 1T_H$	M
Xu et al. [140]	$7T_h + 1T_s + 1T_H + 2T_{pm}$	L	$7T_h + 1T_s + 2T_{pm}$	L
Amin et al. [141]	$4T_h + 1T_{pm}$	H	$7T_h + 2T_s + 4T_{pm}$	L
Awasthi et al. [142]	$4T_h + 4T_{xor}$	M	$4T_h + 4T_{xor}$	M
Tan et al. [143]	$5T_h + 3T_{xor} + 3T_{pm}$	L	$4T_h + 1T_{xor} + 3T_{pm}$	M
Arshad et al. [144]	$6T_h + 9T_{xor} + 3T_{pm}$	L	$9T_h + 6T_{xor} + 3T_{pm} + 1T_{minv}$	L
Yan et al. [145]	$6T_h + 1T_{xor}$	M	$5T_h$	H
Lu et al. [146]	$5T_h + 2T_{pm}$	M	$6T_h + 2T_{pm}$	M
Chaudhry et al. [147]	$4T_h + 2T_{pm}$	M	$3T_h + 2T_{pm}$	H
Mishra et al. [148]	$3T_h + 1T_H$	H	$10T_h + 2T_s$	L
Giri et al. [149]	$5T_h$	H	$1T_{me} + 4T_h$	H
Khan et al. [150]	$6T_h + 2T_{me}$	M	$3T_h + 3T_{me}$	M

formance metrics, however, they add another layer of security that makes the task of an adversary more tougher than for the two-factor authentication schemes. The well designed three-factor authentication schemes which can also satisfy the performance metrics is highly recommended for user authentication in e-Healthcare system.

Chapter 7

PROPOSED MODEL

7.1 Introduction

Chapter 7 is divided in eight sections. First Section 7.1 contains the introduction of the chapter, second contains the comparison of the authentication categories between one-factor, two-factor and three-factor authentication schemes, third contains the proposed hybrid model based on two-factor and three-factor authentication schemes, fourth contains the proposed three-factor authentication scheme with registration phase, login and authentication phase, password update phase and revocation phase. Similarly, fifth Section contains the proposed two-factor authentication scheme containing registration phase, login and authentication phase, password update phase and revocation phase. Section six contains the criteria for ΔT, Section seven contains the emergency handling mechanism, that can be initiated at the time of any emergency by the patient or by the e-Healthcare service provider, and finally Section eight contains the conclusion of the chapter.

7.2 Comparison of Authentication Categories

After thoroughly reviewing several authentication schemes of each category (one-factor, two-factor, three-factor), it has been observed that one-factor authentication schemes are the least expensive one among all the categories in terms of computation cost, communication cost and complexity, but they are also least secured compared to other category schemes. The security of one-factor authentication depends only on the secrecy of the 'ID' and password. The two-factor

authentication schemes provide better security as compared to one-factor authentication schemes at the cost of more delay, high bandwidth, computation cost, communication cost and complexity.

In order to minimize the computation cost, some two-factor authentication schemes do not verify the user identity and password at the end-user, however this increases the communication cost incase the user mistakenly enters the wrong credentials. In that case, a session is rejected by the server after consuming the required bandwidth. This consumed bandwidth can be saved by verifying the user credentials at the smart card end before sending them to the server, and if this mistake occurs in the password update phase, the smart card updates the password at the end-user, whereas the session is rejected by the server at its end due to the false input, and hence the user faces denial of service every time he/she tries to access the TMIS.

Three-factor authentication schemes improve the overall security in a sense that it makes the execution of the attacks harder, as the adversary needs the biometric information of the user in addition to the'ID'and password. Three-factor authentication schemes consume more bandwidth, computation cost and are more complex as compared to other categories. In e-Healthcare, mobility is the most important factor, which enables users to access the healthcare services remotely from their PDAs or cell phones. Two-factor authentication schemes can be implemented using a smart card or a smart phone. Each one has its own advantages and disadvantages. The smart card requires the smart card reader which restricts user mobility as users do not travel with smart card readers in their pockets. On the other hand, the cell phone facilitates user mobility as users keep their cell phones with them all the time.

There is only the algorithm in the smart card that computes user operations for the login purpose and any other data cannot be added to the smart card, whereas a cell phone usually has a lot of applications for different purposes. Any malicious application can record user activity, location

and have access to the cell phone storage, which can compromise user anonymity, untraceability, unlinkability and confidentiality. The mobility of a cell phone comes with a price. There is a tradeoff between mobility and ensured security. In case of a smart card, security is ensured but mobility is restricted whereas in case of a cell phone, mobility is an advantage at the cost of ensured security.

The proposed schemes in the literature treat smart card and cell phone at the same level and claim that the same authentication scheme can be used for both, however it is clear from the above discussion that both of them face different challenges and provide different advantages. All the proposed two-factor authentication schemes are based on the smart card with the claim that they can also be implemented on a cell phone, however the proposed schemes do not use any artifact of the cell phone that can bind them together and take advantage of its mobility.

The same case is with three-factor authentication schemes, as a biometric scanner restricts user mobility whereas a cell phone can compromise ensured security. The results of the study are presented in Table 7.2, Figure 7.1 and 7.2 for better understanding. Table 7.2 presents the properties of authentication categories in tabular form whereas Figure 7.1 and 7.2 presents the properties of authentication categories in graphical form. Figure 7.1 ranks the positive properties of the authentication categories where High represents highest positive rank and Low represents the lowest rank. Similarly, Figure 7.2 represents the negative rank of the authentication categories, where High rank represents the most negative and Low represent the least negative rank of the authentication category. Authentication categories in Table 7.2 are evaluated against the design criteria established in Chapter 3, Section 3.2 and listed in Table 7.1. As a cell phone/smart card is a resource constrained device in terms of processing power, RAM and power source, it requires a lightweight scheme, on the contrary, the three-factor authentication schemes incur more compu-

Table 7.1: Authentication Categories Comparison Metrics

Comparison Metric	Description
B1	User easiness
B2	Scheme complexity
B3	Computation cost
B4	Delay
B5	Communication cost
B6	Mobility in case of smart card/ Biometric scanner
B7	Mobility in case of smart phone
B8	Severity of user compromise
B9	Severity of physician compromise
B10	Provide desired security
B11	Ensure privacy
H	High
M	Medium
L	Low

Table 7.2: Comparison of authentication categories

Category	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11
One-Factor	H	L	L	L	L	–	H	M	H	L	L
Two-Factor	M	M	M	M	M	L	M	M	H	M	M
Three-Factor	L	H	H	H	H	L	M	M	H	H	M

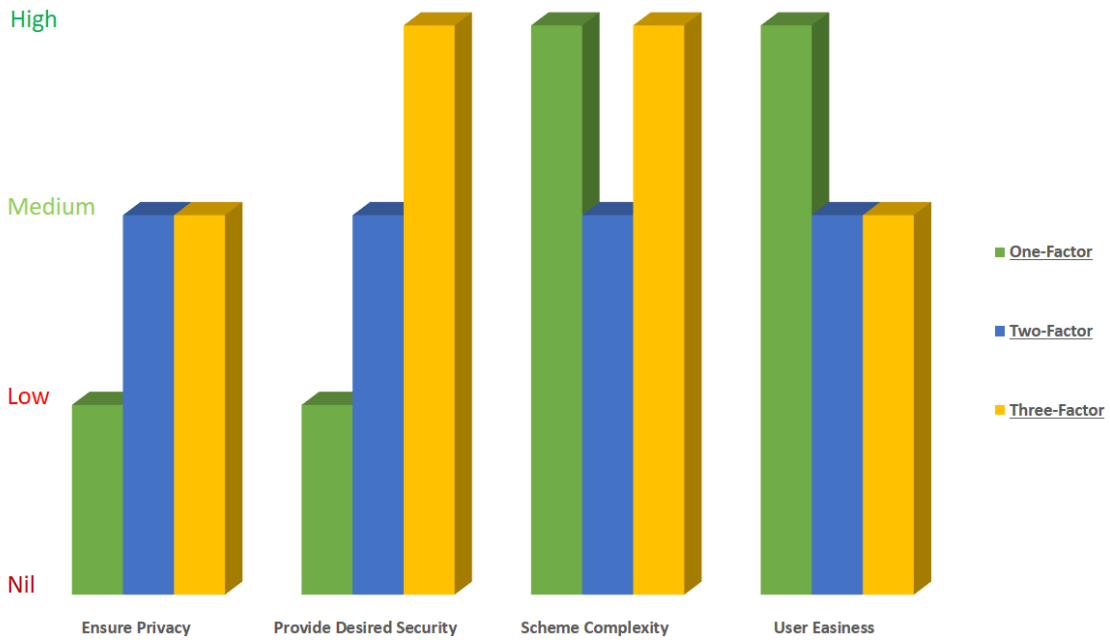

Figure 7.1: Comparison of positive properties of authentication categories

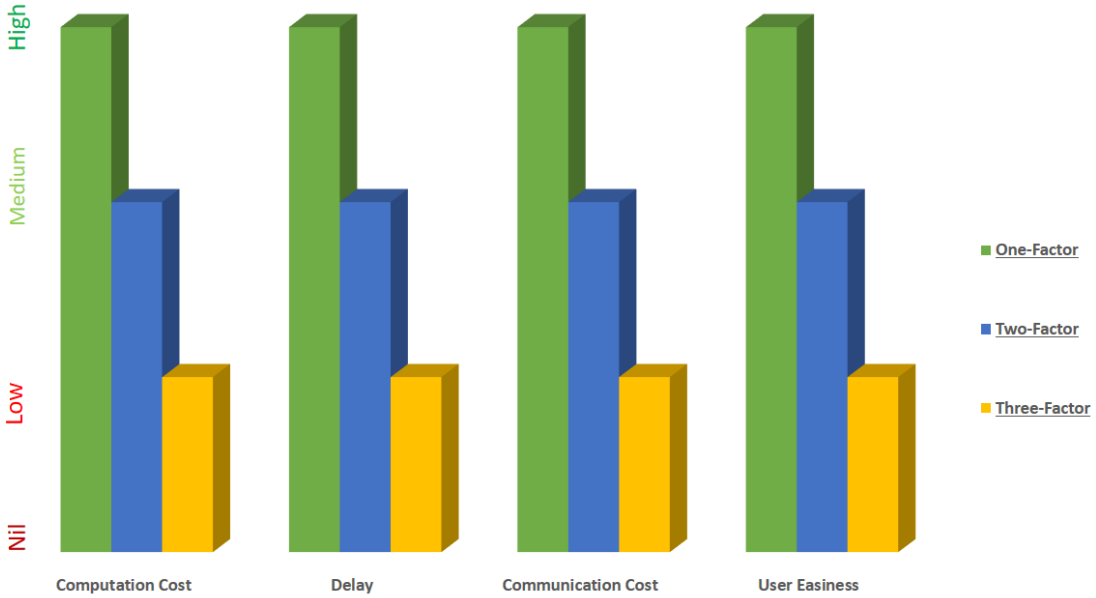

Figure 7.2: Comparison of negative properties of authentication categories

tation cost, delay and bandwidth cost. There is a tradeoff between required resources and desired security. Though three-factor authentication schemes do not provide the desired security but at least they add another layer of security at the cost of more computations and bandwidth.

7.3 User Acceptance For The Third Factor Of Authentication

Cell phone market is moving towards biometric sensor embedded cell phones [153], but still there are millions of cell phones in use and in market that do not have the biometric sensor [153]. Until and unless, only biometric sensor embedded cell phones are left, we need a hybrid solution. Where patient can use his/her non-biometric cell phone to access information on TMIS. The increase in the demand of biometric sensor embedded cell phones reflect that the users are now more comfortable than ever before in using a biometric sensor embedded cell phones [154]. In 2013, only 46 million biometric sensor embedded cell phones were manufactured [153]. The number has sharply increased in recent few years and it is expected that in 2020 there will be 1600 million biometric sensor embedded mobile phone users [153]. In 2014, only 19 percent users had the biometric sensor enabled cell phones [153], the number has gone up sharply and reached to 67 percent this year (2018) [153]. The gradual increase in the biometric sensor embedded cell phones can be seen in Figures 7.3, 7.4 and 7.5. It is expected that in year 2020 all new cell phones will have a biometric sensor embedded in them [153, 155], and in year 2025 all phones will have biometric sensor embedded in them [153, 155], till then we need a hybrid solution to attract more users and make this e-Healthcare revolution globally accepted.

7.4 Proposed Model

We propose a hybrid solution that considers the tradeoff between ensured security, user easiness and availability. Our proposed authentication model is based on the role of the users and presented

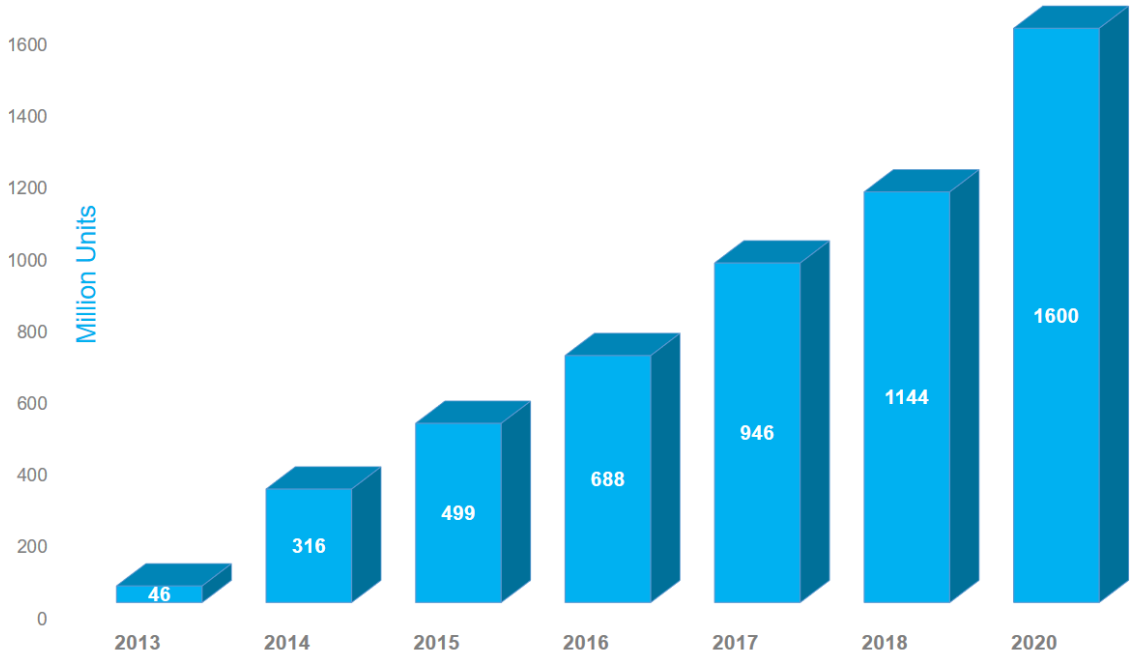

Figure 7.3: Biometric sensor embedded cell phone users

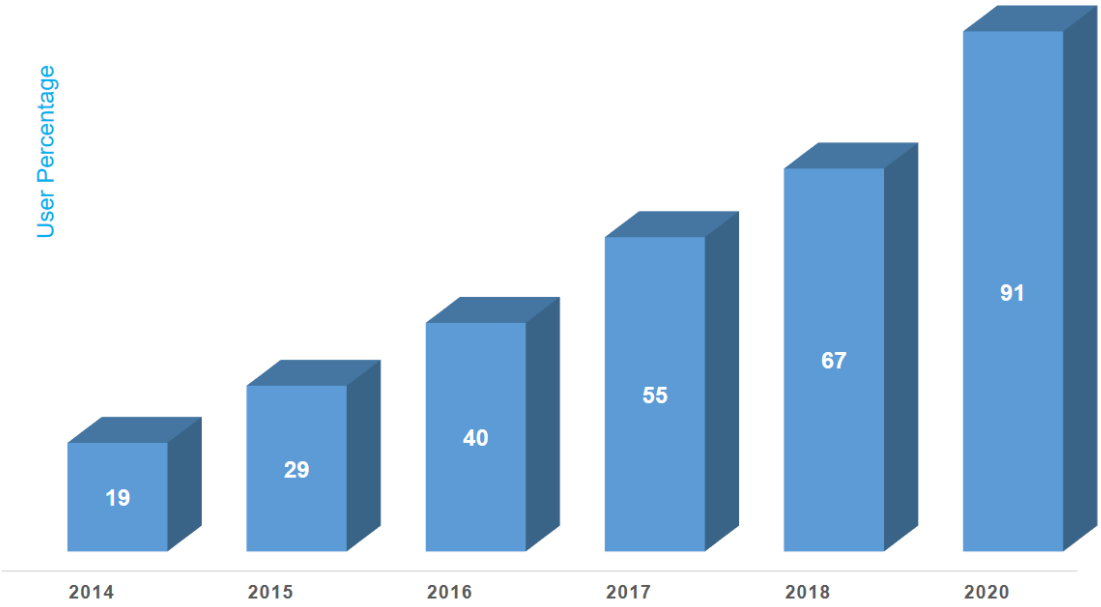

Figure 7.4: Biometric sensor embedded cell phone users's percentage

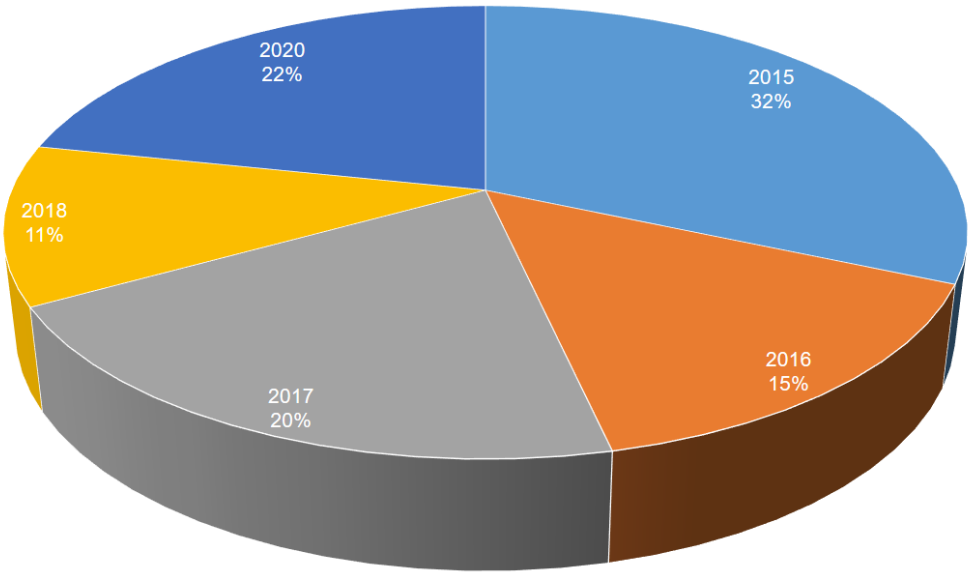

Figure 7.5: Rise of biometric sensor embedded cell phone users in years

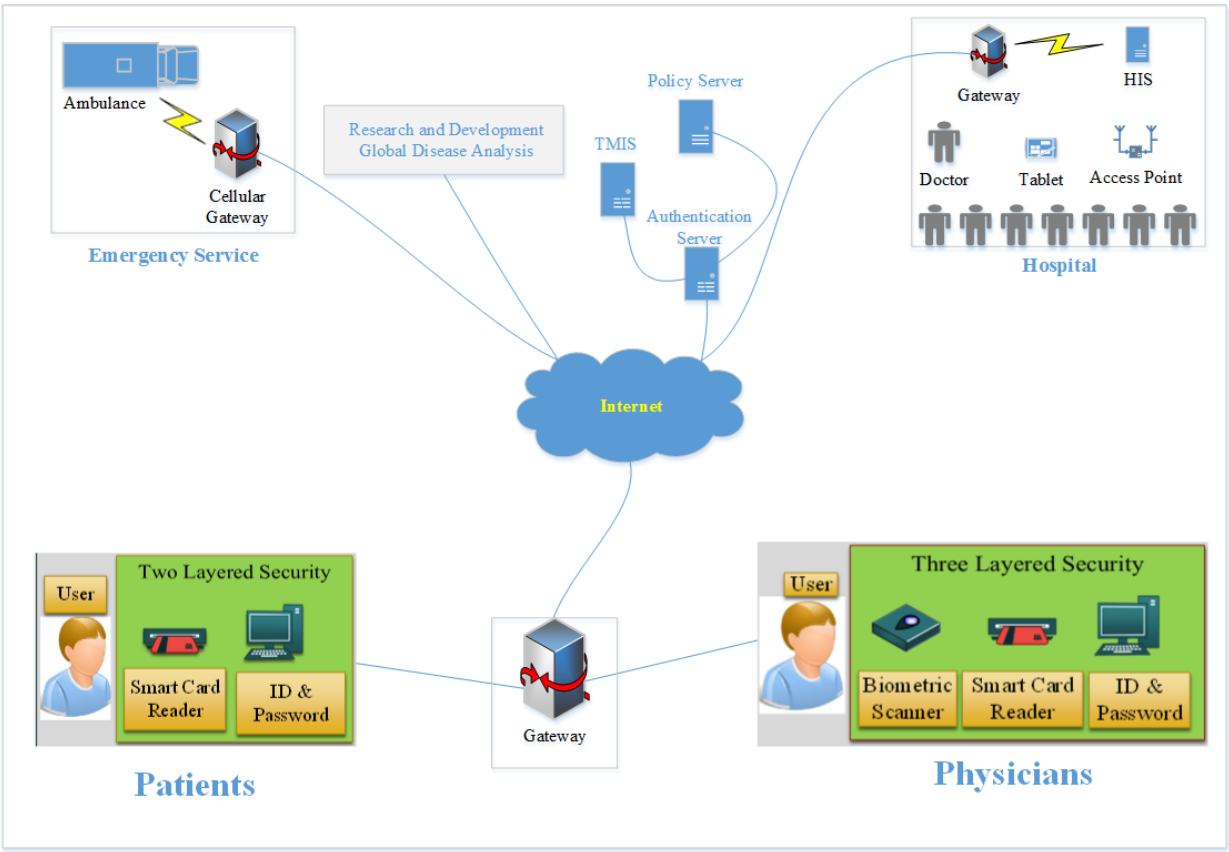

Figure 7.6: Proposed Authentication Model

in Figure 7.6. As physicians have rights to change the information on TMIS, security should be priority in any authentication scheme designed for physicians. On the contrary, patients do not have any right to change the information on TMIS, user easiness should be priority. We proposed a hybrid solution, where physicians will use three-factor authentication scheme and the rest of users will use the two-factor authentication scheme. Generally, physicians have elevated access to the TMIS after successful authentication, and they can prescribe medicine or can change the previous prescribed ones. In contrast, patients can only view the information, as they do not have the authority to change any information on the TMIS. As patients do not have the authority to change anything on the TMIS, so the integrity of the information on TMIS cannot be compromised. This becomes very critical when the authentication information of the physician is compromised, in that case, the adversary will be able to compromise the integrity of the information on the TMIS, in addition to confidentiality, anonymity and privacy. This requires more security measures for the physicians than the ordinary users of e-Healthcare.

To elaborate the hybrid solution advantages over the existing schemes, we take the example of a diabetic patient. Diabetic patients inject insulin to control sugar level in their blood. The amount of injecting insulin depends on the sugar level, high sugar level demands high dose of insulin and vice versa. In e-Healthcare, patient's blood sugar is monitored regularly and the physician prescribes the amount of insulin dose on the basis of the blood sugar results.

Consider that the user credentials are compromised by an adversary, in that case the adversary will be able to see the blood sugar results and the corresponding insulin dose. The adversary cannot change the test results and the prescribed dose of insulin as he/she does not have the permission to change anything on the TMIS.

Now, consider the case where the physician's credentials are compromised by the adversary, this

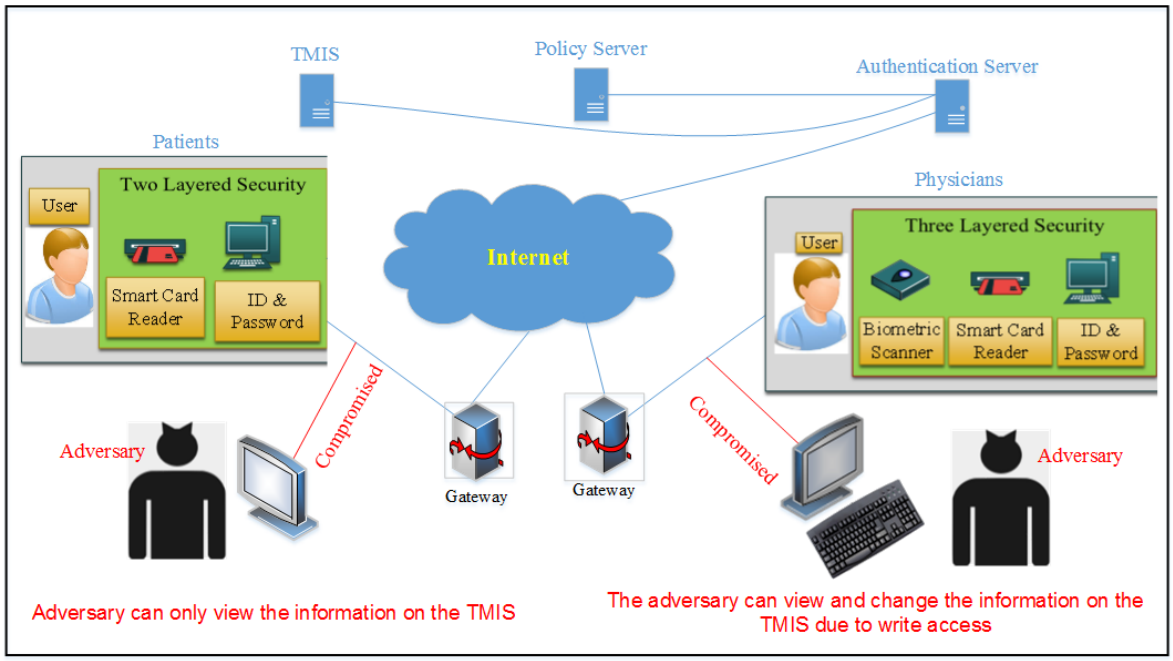

Figure 7.7: Severity comparison of an authentication breach between patients and physicians

becomes critical because now adversary can also change the amount of insulin dose for the user. The user does not know anything about the compromise and takes the dose as he/she sees on the TMIS. The wrong dose can severely affect the blood sugar level and can even claim the life of of the patient. From this example, it is clear that the physician's credentials compromise affects the system and the patient more severely than any other user's credentials compromise. Figure 7.7 shows the severity comparison between the patients and the physicians in case of any authentication breach. It can be observed in Figure 7.7 that only availability, confidentiality and privacy of the patient can be compromised in case of any breach due to patient's authentication credentials, whereas any authentication breach due to physician's authentication credentials, the integrity of the information can also be comprised in addition to availability, confidentiality and privacy.

This demands more security measures for physician authentication, therefore we recommend three-factor authentication scheme for the physicians and two-factor authentication scheme for

the rest of the users. Current authentication schemes holds the same criteria for physicians and for rest of the users of e-Healthcare. Two-factor authentication schemes are more efficient but fails to ensure the desired security, whereas three-factor authentication schemes are close to approach the desired security at the cost of efficiency. Our proposed approach meets the requirements of both parties, as users need efficiency and physicians need desired security to make the system successful and globally accepted.

Mobility is another factor which restricted the use of three-factor authentication schemes for mobile users in recent past, as mobile phones with biometric sensors were very rare and expensive [153, 156, 92], due the fact of their poor performance and high false rejection rate [157], whereas it is the main objective of the e-Healthcare provider to facilitate the user mobility. Similarly, users do not keep a smart card reader with them when they are mobile, therefore smart card is not an efficient solution to facilitate user mobility. To facilitate user mobility, smart card can be replaced with a cell phone as a second layer of security because users always tend to keep their cell phones with them, and to reap the benefits of three-factor authentication schemes in mobility, users should have a biometric scanner with them or the biometric sensor should be embedded in the smart phone. Thus, it was comparatively difficult to provide the desired security (three-factor authentication scheme) to mobile users in recent past.

This demands a tradeoff between the desired security and the available resources and also the tradeoff between the mobility and the ensured security. As cell phones ensure less security as compared to a smart card or biometric scanner. Our proposed solution is the best for these kind of situations, as it is very hard to provide the required resources to every user, and it is also very hard for the user to manage multiple resources in mobility. So, it is expected that in the future, we will mostly encounter hybrid solutions, where physicians will use more secure and

resource demanding authentication schemes, and ordinary users will use less secure and less resource demanding authentication schemes as required.

7.5 e-Healthcare Authentication Mechanism

e-Healthcare authentication mechanism consists of five phases as shown in figure7.8. Registration phase is the first phase, where users register their selves for e-Healthcare services. This phase occurs only once and elaborated in Figure 7.9, in this phase, service providers gather users information for their record, so that users can be authenticated later for e-Healthcare services. After successful registration, users request offered services from service provider. The service providers authenticate the users before granting access to the offered resources as shown in Figure 7.10. This request phase is the second phase while the request authentication is the third phase, as both these phases are connected with each other and also occur together, they can be combined and referred as one. Service provider approves or disapproves the login request after verifying the user information. For security purposes, users are required to change / update their password regularly, password update phase provides users an option to update their password when they deem necessary or according to the policies of the service providers. User can also revoke his/ her registration incase of lost / stolen authentication credentials or authenticated device.

7.6 Proposed Three Factor Authentication Scheme

Our proposed three factor authentication scheme has five phases.

- Registration Phase
- Login Phase
- Authentication Phase
- Password Update Phase

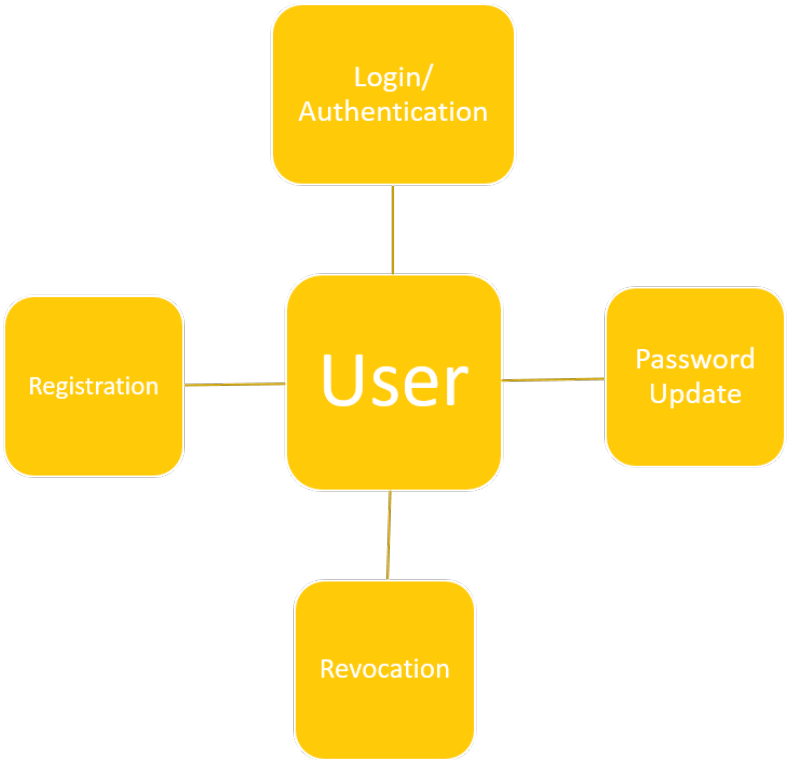

Figure 7.8: e-Healthcare Authenticationion Mechanism

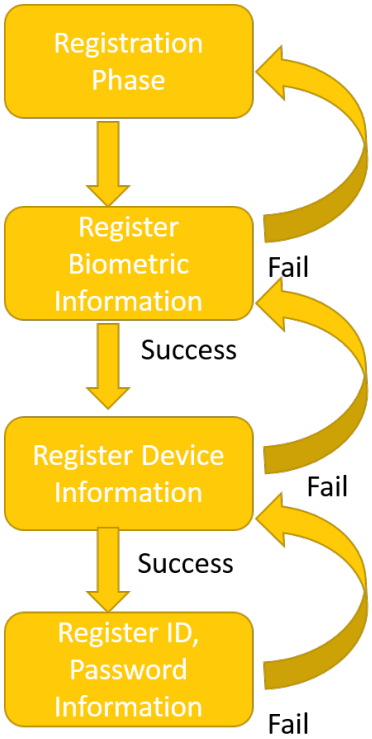

Figure 7.9: e-Healthcare Registration Phase

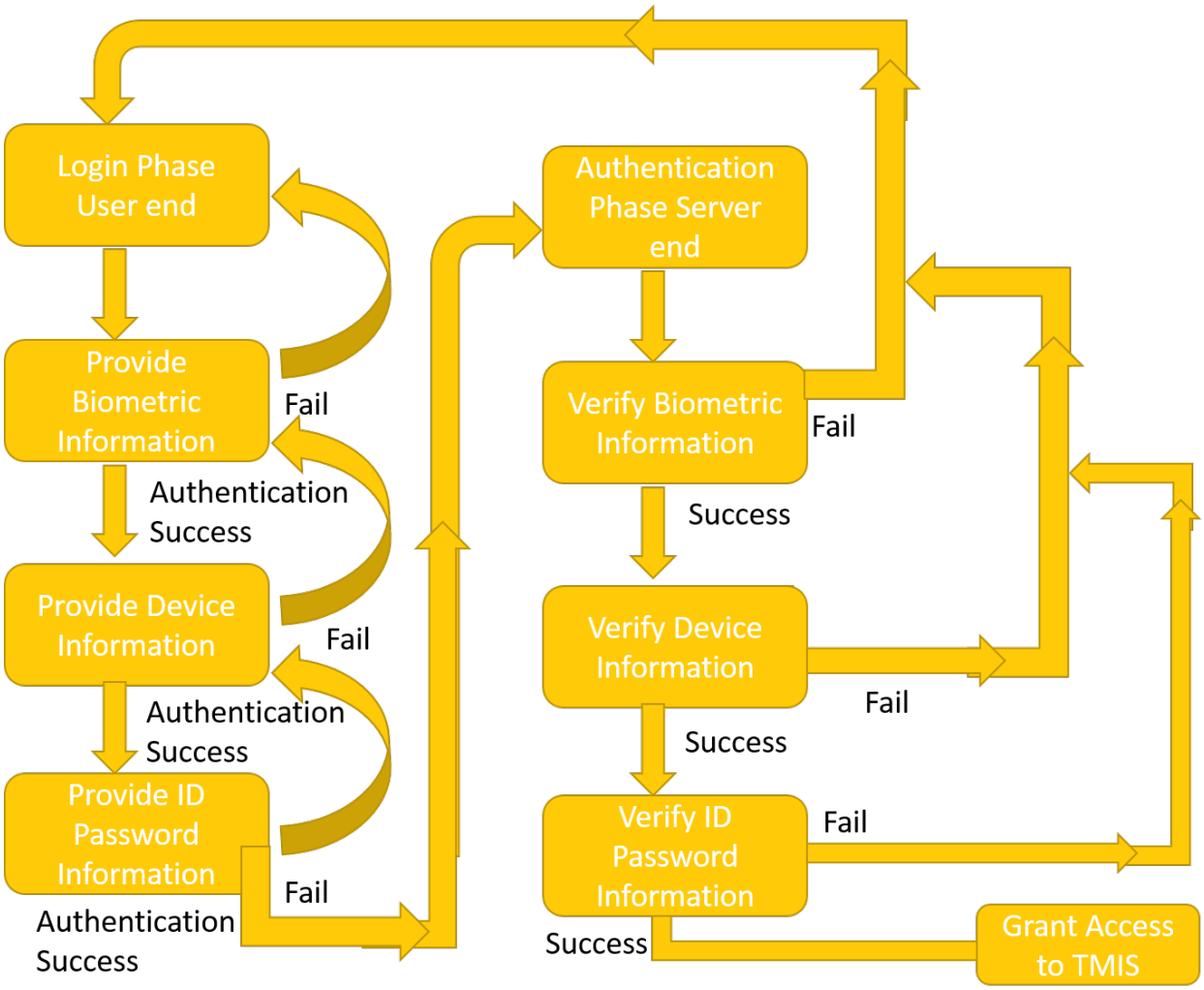

Figure 7.10: e-Healthcare Login / Authentication Mechanism

- Revocation Phase

7.6.1 Registration Phase

In registration phase, the user first downloads the e-Healthcare provider application from a legitimate platform for accessing the services provided by the service provider. On downloading the application, the cell phone also downloads the server's public key S_{pub}, functions such as hash function $h(.)$, bio-hash function $H(.)$, encryption E_{key} and decryption functions D_{key}. The downloaded keys and functions are the part of the application and application cannot execute properly without these keys and functions.

In this phase user registers with the service provider as a physician. In the 1^{st} step, user registers his/her biometric information B_i by imprinting his/her fingerprint, cell phone computes F_i=$H(B_i)$ of provided biometric information. B_i is the provided biometric information and F_i is the bio-hash of the given input. In the 2^{nd} step, user keys his/her 'ID', password 'PWD' and trusted cell phone number 'N'. Cell phone application on receiving the said input computes $RPWD = h(r||PWD)$, where 'r' is a random nonce. Cell phone also computes $S_{pub}(ID, N, RPWD, F_i, T_{uc})$, where T_{uc} is the current timestamp of the user and S_{pub} is the public key of the server. Cell phone transmits the following information to server:

- $U \rightarrow S$ = $S_{pub}(ID, N, RPWD, F_i, T_{uc})$

On receiving information from the user, the server decrypts the received information using its private key S_{pri} and extract the 'ID', cell phone number 'N' of the registering user, password of the user hashed with a random nonce '$RPWD$', bio-hash of the user's biometric information F_i and the registration timestamp T_{uc}. At first, the server verifies the $\Delta T = (T_{sc} - T_{uc})$, where T_{sc} is the current timestamp at the server end, ΔT should be in the permissible range to thwart

any replay attack. Server then verifies the format of the 'ID', the cell phone number 'N' and also verifies uniqueness of them and computes the following:

$S_{pri}(S_{pub}(ID, N, RPWD, F_i, T_{uc}))$

$P = h(R||ID)$

$Q = P \oplus RPWD$

$Y = h(P||RPWD||ID)$

$RID = S_{pub}(ID||R)$

$K = R \oplus RPWD$

where 'R' is a random nonce generated at server end and S_{pub} is the public key of the server. After these computations server stores 'RID' in its registration database and sends the verification code 'K' through GSM message to the user's given cell phone number for verification purpose. On receiving the verification message, the user application first retrieves 'R' by computing $R = K \oplus RPWD$, then asks the user device for its serial number 'Ser' and computes $S_{pub}(R||Ser||T_{uc})$. The application then sends the computed parameter to the server. Server decrypts $S_{pri}(S_{pub}(R||Ser||T_{uc}))$ the response from the user, first verifies the $\Delta T = (T_{sc} - T_{uc})$ and then the random nonce 'R', where T_{uc} is the current timpestamp at the user end, T_{sc} is the current timpestamp at the server end and ΔT is the permissible range of time after which the message will expire. On the successful verification, the server stores 'Ser' (serial number of the device) and sends the following to the user.

- $S \rightarrow U$ = $S_{pri}(Q, RID, Y, T_{sc})$

On receiving the above information from server, the user first decrypts the message by using the server's public key S_{pub}. After successful decryption the user verifies the ΔT=$(T_{uc} - T_{sc})$, where T_{uc} is the current timestamp at the user end and T_{sc} is the current timestamp at the server end, ΔT

should be in the permissible range to thwart any replay attack. The successful decryption verifies the authenticity of the message that it came from the server and cannot come from anywhere else as no one can have server's private key S_{pri}. After verifying the authenticity, the user computes $Z = h(ID||PWD) \oplus r$ and saves the output in its database and discards all other values except these (F_i, Q, RID, Y, Z).

7.6.2 Login Phase

This phase is more important than the registration phase in respect of communication cost, computation cost and delay, because registration phase occurs once whereas this phase occurs whenever a user attempts to access the services provided by the e-Healthcare provider. To access the services, user presents its biometric information by placing his/her registered finger on the cell phone fingerprint sensor. The e-Healthcare provider application installed in the cell phone computes $F_i = H(B_i)$ and compares it with the stored one in its database. On successful verification, application asks for the associated username '(ID)' and password 'PWD'. User keys his/her 'ID' and password 'PWD', on receiving the desired information, the user's application first retrieves the random nonce 'r' and computes other parameters by performing the following operations:

$r = Z \oplus h(ID||PWD)$

$RPWD = h(r||PWD)$

$P = Q \oplus RPWD$

$Y = h(P||RPWD||ID)$

Where 'r' is the retrieved nonce and 'P' is the shared secret between user and server and never traveled on the communication channel during the registration phase instead $Q = P \oplus RPWD$ was transmitted. Cell phone matches the computed 'Y' with the stored one to verify the given

'ID'and password 'PWD'. If it does not match, the application ends the current login session otherwise application computes $J_u = h(T_{uc}||P)$, where T_{uc} is the current timestamp at user end. User sends the following information to the server.

- $U \rightarrow S$ = $S_{pub}(RID, J_u, T_{uc}, F_i)$

7.6.3 Authentication Phase

In this phase server authenticates the user on the basis of the given information by the user. On receiving information $S_{pub}(RID, J_u, T_{uc}, F_i)$ from the user, the server first decrypts it with its private key S_{pri} and retrieves (RID, J_u, T_{uc}, F_i), server then verifies the freshness of the message by computing $\Delta T = (T_{sc} - T_{uc})$, once freshness is guaranteed server verifies the biometric information F_i from its database. If the verification of freshness of the message or the biometric information F_i fails, the server terminates the current session or otherwise computes the following:

$S_{pri}(S_{pub}(ID||R))$ Retrieves user 'ID' and server generated nonce 'R'

$P = h(S_{pri}||ID)$ Retrieves shared secret 'P'

$J_u^{'}$=h($T_{uc}||P$)

$RID^{'}$=$S_{pri}(ID||R)$

J_s=$E_p(RID^{'}, J_u^{'}, T_{sc})$ Encryption using shared secret 'P' as symmetric encryption key

Where 'P' is the shared secret and 'R' is the retrieved nonce generated at server end. After computing '$J_u^{'}$' server checks its equivalency with the received one from the user. Equivalency implies that the user is a legitimate user of the TMIS. If equivalency does not hold, server terminates the current session. If equivalency holds then server computes $RID^{'}$, J_s and sends it to user so that user can also authenticate the server. After performing the above mentioned operations, server

sends the following information to the user:

- $S \rightarrow U$ = (J_s, T_{sc})

On receiving the response message from the server, the user performs the following operations to authenticate the server:

$D_p(J_s)$=$D_p(E_p(RID^{'}, J_u^{'}, T_{sc}))$ Decryption using shared secret 'P' as symmetric decryption key

ΔT=(T_{uc}-T_{sc})

Check the equivalency of $J_u^{'}$=J_u , if does not hold terminate the session otherwise verify the equivalency of stored RID with the received $RID^{'}$, if does not hold terminate the session, otherwise the legitimacy of the server is achieved. After the mutual authentication user and server both compute the session key as follows: S_k=$h(P||T_{uc}||T_{sc})$

Cell phone first verifies that ΔT is within the permissible range, then checks the equivalency of received $J_u^{'}$ with the computed one at its end. If ΔT is not within the permissible range or $J_u^{'}$ does not match, cell phone application terminates the current session or otherwise server identity is verified along with message freshness . After verifying the server identity, user computes the session key S_k for current session. Server also computes the session key S_k at its end. Our authentication scheme does not only successfully achieves the mutual authentication but it also verifies the legitimacy of the user device. For the verification of the user device, server sends a verification code 'K' to the registered number 'N' of the user. On receiving the verification code 'K' from server, user retrieves 'R' by computing $R = K \oplus RPWD$, retrieves the device's serial number Ser, computes $S_{pub}(R||Ser||T_{uc})$ and sends it to the server. After receiving the input from user, the server decrypts the message using its private key S_{pri} and verifies the 'R' and the

received serial number with with the stored ones. On successful verification of both, the server grants the access to the TMIS.

7.6.4 Password Update Phase

In this phase, the user updates his/ her password, the password should be changed and updated at both ends in an efficient manner. The password change should be properly communicated to the server before updating at the user end. Consider a scenario in which user changes his/ her password and fails to communicate the update to the server due to the loss/ unavailability of the communication channel. In such a situation, the user and server will have a different password, hence he/ she will not be able to login to the server and will face denial of service.

Our proposed password update mechanism updates the user password at the user end after getting approval from the server. In password update phase, the user first logs in to the server and requests to initiate the password change mechanism. The password update wizard will ask the user to provide a new password $PWD^{'}$, on receiving the input from the user the wizard computes $RPWD^{'}$=$h(r^{'}||PWD^{'})$, where '$r^{'}$' is a new random nonce. The update wizard computes $S_{pub}(RPWD^{'}, T_{uc})$, where T_{uc} is the current timestamp of the user and S_{pub} is the public key of the server. Cell phone transmits this computed information to the server:

- $U \rightarrow S$ = $S_{pub}(RPWD^{'}, T_{uc})$

On receiving the above information from the user, the server decrypts the received information using its private key S_{pri} and extracts the updated password $RPWD^{'}$ of the user hashed with a new random nonce '$r^{'}$' and the user timestamp. At first, the server verifies the ΔT =(T_{sc}-T_{uc}), where T_{sc} is the current timestamp at the server end, ΔT should be in the permissible range to thwart any replay attack. Server then generates a new random nonce '$R^{'}$' and compute $K^{'}$ =R$^{'}$

$\oplus RPWD$ and sends the verification code '$K^{'}$' to the user's registered cell phone number through GSM channel, On receiving the verification code '$K^{'}$' the application retrieves '$R^{'}$' by computing $R^{'} = K^{'} \oplus RPWD$. The application also retrieves the serial number Ser of the device, then computes $S_{pub}(R^{'}||Ser||T_{uc})$ and sends it to the server. Server decrypts $S_{pri}(S_{pub}(R^{'}||Ser||T_{uc}))$ the response message from the user. The user then verifies the ΔT =(T_{sc}-T_{uc}), serial number Ser of the device and random nonce '$R^{'}$'. On successful verification, the server computes the following and sends to the user:

$S_{pri}(S_{pub}(RPWD^{'}, T_{uc}))$

$P^{'} = h(R^{'}||ID)$

$Q^{'}$=$P^{'} \oplus RPWD^{'}$

$Y^{'}$=$h(P^{'}||RPWD^{'}||ID)$

- $S \rightarrow U$ = $S_{pri}(Q^{'}, Y^{'}, T_{sc})$

On receiving the information from the server, the cell phone first decrypts the message by using the server's public key S_{pub}, then verifies the ΔT =(T_{uc}-T_{sc}). The successful decryption using server's public key S_{pub} verifies the authenticity of the message that it came from the server and cannot come from anywhere else. After verifying the authenticity of the server, the user computes $Z^{'}$=$h(ID||PWD^{'}) \oplus r$ and saves the new computed values of $Q^{'}$, $Y^{'}$ and $Z^{'}$ and discards the previous computed ones.

In password update phase, the service provider application installed in cell phone computes a new random 'r' that is very critical in computing the shared secret 'P', therefore frequent update of user password becomes very important.Therefore, in proposed model, the server will force the user to update his/her password after every 30 days or after every 50 successful authentication requests, whichever comes first. This will be very helpful in mitigating online password guessing

attack, offline guessing attack, replay attack and will also protect user anonymity against attacks on user identity.

The complete flow of the proposed three-factor authentication scheme is presented in Table 7.4 and the notations used in the scheme are given in Table 7.3 for better understanding.

Table 7.3: Description of used notations in proposed schemes

Notation	Description
B_i	User biometric information
F_i	Bio-hash of given biometric information
ID	User chosen identification/ username
PWD	User chosen password
N	Cell phone number of the user
Ser	Serial number of the user device
$RPWD$	Hash of user password after concatenated with 'r' for insider attack protection
R	Random nonce generated at server end
r	Random nonce generated at user end
P	Shared secret
RID	Encrypted user ID after concatenated with 'R', securing user ID for anonymity
Y	Cell phone matches to verify the user ID and PWD during login phase
S_{pri}	Server's private key
S_{pub}	Server's public key
S_k	Session key
E_p	Encryption function using shared secret P as encryption key
D_p	Decryption function using shared secret P as decryption key
K	Verification code sent through GSM
T_{uc}	Current time at user end
T_{uc}	Current time at server end
ΔT	Permissible time after which the message will expire

Table 7.4: Proposed three-factor authentication scheme

Phase	User	TMIS
Registration	F_i=$H(B_i)$	
	'ID', 'PWD'	
	$RPWD = h(r\|\|PWD)$	
	$S_{pub}(ID, N, RPWD, F_i, T_{uc})$	
	U $\xrightarrow{S_{pub}(ID, N, RPWD, F_i, T_{uc})}$ S	
		$S_{pri}(S_{pub}(ID, N, RPWD, F_i, T_{uc}))$
		$T = (T_{sc} - T_{uc})$
		$P = h(R\|\|ID)$
		$Q = P \oplus RPWD$
		$Y = h(P\|\|RPWD\|\|ID)$
		$RID = S_{pub}(ID\|\|R)$
		$K = R \oplus RWPD$
		U $\xleftarrow{\text{Verification Code '}K\text{' Through GSM}}$ S
	$R = K \oplus RWPD$	
	Retrieves serial number	
	'Ser' of the device	
	$S_{pub}(R\|\|Ser\|\|T_{uc})$	
	U $\xrightarrow{S_{pub}(R\|\|Ser\|\|T_{uc})}$ S	
		$S_{pri}(S_{pub}(R\|\|Ser\|\|T_{uc}))$
		ΔT =(T_{sc}-T_{uc})
		Verify the random none 'R'
		U $\xleftarrow{S_{pri}(Q, RID, Y, T_{sc})}$ S
	$S_{pub}(S_{pri}(Q, RID, Y, T_{sc}))$	
	ΔT =(T_{uc}-T_{sc})	
	$Z = h(ID\|\|PWD) \oplus r$	
Login and Authentication	F_i = $F_i^{'}$= $H(B_i)$	
	r=$Z \oplus h(ID\|\|PWD)$	
	$RPWD = h(r\|\|PWD)$	
	$P = Q \oplus RPWD$	

Table 7.4: Proposed three-factor authentication scheme

Phase	User	TMIS
	$Y = h(P\|\|RPWD\|\|ID)$	
	$J_u = h(T_{uc}\|\|P)$	
	$S_{pub}(RID, J_u, T_{uc}, F_i)$	
	$\text{U} \xrightarrow{S_{pub}(RID, J_u, T_{uc}, F_i)} S$	
		$S_{pri}(S_{pub}(RID, J_u, T_{uc}, F_i))$
		$\Delta T = (T_{sc} - T_{uc})$
		Check if
		F_i=F_i (Stored in DB)
		$S_{pri}(S_{pub}(ID\|\|R))$
		$P = h(R\|\|ID)$
		$J_u^{'}$=h($T_{uc}\|\|P$)
		Check if
		$J_u^{'}$=J_u
		$RID^{'}$= $S_{pri}](ID\|\|R)$
		J_s=$E_p(RID^{'}, J_u^{'}, T_{cs})$
		$\text{U} \xleftarrow{(J_s, T_{cs})} S$
	$D_p(E_p(RID^{'}, J_u^{'}, T_{sc}))$	
	ΔT =(T_{uc}-T_{sc})	
	Check if	
	$J_u^{'}$=J_u	
	Check if	
	RID=$RID^{'}$	
	$S_k = h(P\|\|T_{uc}\|\|T_{sc})$	$S_k = h(P\|\|T_{uc}\|\|T_{sc})$
Password Update	$RPWD^{'}$=$h(r^{'}\|\|PWD^{'})$	
	$S_{pub}(RPWD^{'}, T_{uc})$	
	$\text{U} \xrightarrow{S_{pub}(RPWD^{'}, T_{uc})} S$	
		$S_{pri}(S_{pub}(RPWD^{'}, T_{uc}))$
		ΔT=(T_{sc}-T_{uc})
		$K^{'} = R^{'} \oplus RWPD$

Table 7.4: Proposed three-factor authentication scheme

Phase	User	TMIS
		U $\xleftarrow{\text{Verification Code '}K^{'}\text{' Through GSM}}$ S
	$R^{'} = K^{'} \oplus RWPD$	
	Retrieves serial number	
	'Ser' of the device	
	$S_{pub}(R^{'}\|\|Ser\|\|T_{uc})$	
	U $\xrightarrow{S_{pub}(R^{'}\|\|Ser\|\|T_{uc})}$ S	
		$S_{pri}(S_{pub}(R^{'}\|\|Ser\|\|T_{uc}))$
		ΔT=(T_{sc}-T_{uc})
		Verify Random nonce '$R^{'}$' and
		serial number 'Ser' of the device
		$P^{'} = h(R^{'}\|\|ID)$
		$Q^{'}$=$P^{'} \oplus RPWD^{'}$
		$Y^{'}$=$h(P^{'}\|\|RPWD^{'}\|\|ID)$
		U $\xleftarrow{S_{pri}(Q^{'}, Y^{'}, T_{sc})}$ S
	$S_{pub}(S_{pri}(Q^{'}, Y^{'}, T_{sc})$	
	ΔT=(T_{uc}-T_{sc})	
	$Z^{'}$=$h(ID\|\|PWD^{'}) \oplus r$	

7.6.5 Revocation Phase

Users only go through from this phase when they want to revoke their registration due to registered device loss/stolen, 'ID' compromise or password compromise. For an efficient revocation mechanism, user must provide his/her backup cell phone number or email address which he/she can access at an appropriate time accordingly. The backup cell phone number or email address must be provided by the user when he/she login for the first time, the application will not offer its services until backup cell phone number or email address is provided. Incase of device loss, the

user downloads the application on any device and goes to the revocation section, this section asks the username, password and registered cell phone number of the user and encrypts them with the server's public key S_{pub} and sends it to the server. Server upon receiving the message from user, decrypts the message using its private key S_{pri}. Server verifies the 'ID', password and cell phone number, after successful verification, the server demands the backup cell phone number or email address previously provided by the user so that a verification code can be sent to the user. On providing the valid backup cell phone number or email address, the server sends the verification code to the provided input. On receiving the verification code user encrypts the verification code with server's public key S_{pub} and sends it to the server, server upon receiving the message from user decrypts the message using its private key S_{pri}. Server verifies the verification code by matching it with the sent one and on successful verification revokes/terminates the user account so that it cannot be misused by anyone. All the messages sent to user or server contain timestamp so that the freshness of every message can be guaranteed.

7.7 Proposed Two Factor Authentication Scheme

The proposed two-factor authentication is very similar to the proposed three-factor authentication scheme with few minor differences. As we have proposed a two-factor authentication scheme for the patients in our hybrid model, we have removed the biometric information verification from the proposed two-factor authentication scheme. The scheme does not also dully verify the device identity by sending the verification code to the patient, a verification code is sent to the patient only when he/she wants to change his/her password, revokes his/her identity or when bypasses authentication mechanism incase of emergency. Our proposed two-factor authentication scheme also have five phases.

- Registration Phase

- Login Phase
- Authentication Phase
- Password Update Phase
- Revocation Phase

7.7.1 Registration Phase

In registration phase, the user first downloads the e-Healthcare provider application from a legitimate platform for accessing the services provided by the service provider. On downloading the application, the cell phone also downloads the server's public key S_{pub}, functions such as hash function $h(.)$, bio-hash function $H(.)$, encryption E_{key} and decryption functions D_{key}. The downloaded keys and functions are the part of the application and application cannot execute properly without these keys and functions.

In this phase user registers with the service provider as a physician. In the 1^{st} step, user keys his/her 'ID', password 'PWD' and trusted cell phone number 'N'. Cell phone application on receiving the said input computes $RPWD = h(r||PWD)$, where 'r' is a random nonce. Cell phone also computes $S_{pub}(ID, N, RPWD, T_{uc})$, where T_{uc} is the current timestamp of the user and S_{pub} is the public key of the server. Cell phone transmits the following information to server:

- $U \rightarrow S$ = $S_{pub}(ID, N, RPWD, T_{uc})$

On receiving information from the user, the server decrypts the received information using its private key S_{pri} and extract the 'ID', cell phone number 'N' of the registering user, password of the user hashed with a random nonce '$RPWD$' and the registration timestamp T_{uc}. At first, the server verifies the $\Delta T = (T_{sc} - T_{uc})$, where T_{sc} is the current timestamp at the server end, ΔT should be in the permissible range to thwart any replay attack. Server then verifies the format

of the 'ID', the cell phone number 'N' and also verifies uniqueness of them and computes the following:

$S_{pri}(S_{pub}(ID, N, RPWD, T_{uc}))$

$P = h(R||ID)$

$Q = P \oplus RPWD$

$Y = h(P||RPWD||ID)$

$RID = S_{pub}(ID||R)$

$K = R \oplus RPWD$

where 'R' is a random nonce generated at server end and S_{pub} is the public key of the server. After these computations server stores 'RID' in its registration database and sends the verification code 'K' through GSM message to the user's given cell phone number for verification purpose. On receiving the verification message, the user application first retrieves 'R' by computing $R = K \oplus RPWD$, then asks the user device for its serial number 'Ser' and computes $S_{pub}(R||Ser||T_{uc})$. The application then sends the computed parameter to the server. Server decrypts $S_{pri}(S_{pub}(R||Ser||T_{uc}))$ the response from the user, first verifies the $\Delta T = (T_{sc} - T_{uc})$ and then the random nonce 'R', where T_{uc} is the current timpestamp at the user end, T_{sc} is the current timpestamp at the server end and ΔT is the permissible range of time after which the message will expire. On the successful verification, the server stores 'Ser' (serial number of the device) and sends the following to the user.

- $S \rightarrow U$ = $S_{pri}(Q, RID, Y, T_{sc})$

On receiving the above information from server, the user first decrypts the message by using the server's public key S_{pub}. After successful decryption the user verifies the ΔT=$(T_{uc} - T_{sc})$, where T_{uc} is the current timestamp at the user end and T_{sc} is the current timestamp at the server end, ΔT

should be in the permissible range to thwart any replay attack. The successful decryption verifies the authenticity of the message that it came from the server and cannot come from anywhere else as no one can have server's private key S_{pri}. After verifying the authenticity, the user computes $Z = h(ID||PWD) \oplus r$ and saves the output in its database and discards all other values except these (Q, RID, Y, Z).

7.7.2 Login Phase

This phase is more important than the registration phase in respect of communication cost, computation cost and delay, because registration phase occurs once whereas this phase occurs whenever a user attempts to access the services provided by the e-Healthcare provider. To access the services, user keys his/her 'ID' and password 'PWD', on receiving the desired information from user the user's application first retrieves the random nonce 'r' and computes other parameters by performing the following operations:

$r = Z \oplus h(ID||PWD)$

$RPWD = h(r||PWD)$

$P = Q \oplus RPWD$

$Y = h(P||RPWD||ID)$

Where 'r' is the retrieved nonce and 'P' is the shared secret between user and server and never traveled on the communication channel during the registration phase instead $Q = P \oplus RPWD$ was transmitted. Cell phone matches the computed 'Y' with the stored one to verify the given 'ID'and password 'PWD'. If it does not match, the application ends the current login session otherwise application computes $J_u = h(T_{uc}||P)$, where T_{uc} is the current timestamp at user end. User sends the following information to the server.

- $U \rightarrow S$ = $S_{pub}(RID, J_u, T_{uc})$

7.7.3 Authentication Phase

In this phase server authenticates the user on the basis of the given information by the user. On receiving information $S_{pub}(RID, J_u, T_{uc})$ from the user, the server first decrypts it with its private key S_{pri} and retrieves $(RID, J_u, T_{uc}$, server then verifies the freshness of the message by computing $\Delta T = (T_{sc} - T_{uc})$, once freshness is guaranteed, then the server verifies the other presented parameters. If the verification of freshness of the message fails, the server terminates the current session or otherwise computes the following:

$S_{pri}(S_{pub}(ID||R))$ Retrieves user 'ID' and server generated nonce 'R'

$P = h(S_{pri}||ID)$ Retrieves shared secret 'P'

$J_u^{'}$=h($T_{uc}||P$)

$RID^{'}$=$S_{pri}(ID||R)$

J_s=$E_p(RID^{'}, J_u^{'}, T_{sc})$ Encryption using shared secret 'P' as symmetric encryption key

Where 'P' is the shared secret and 'R' is the retrieved nonce generated at server end. After computing '$J_u^{'}$' server checks its equivalency with the received one from the user. Equivalency implies that the user is a legitimate user of the TMIS. If equivalency does not hold, server terminates the current session. If equivalency holds then server computes $RID^{'}$, J_s and sends it to user so that user can also authenticate the server. After performing the above mentioned operations, server sends the following information to the user:

- $S \rightarrow U$ = (J_s, T_{sc})

On receiving the response message from the server, the user performs the following operations to authenticate the server:

$D_p(J_s)$=$D_p(E_p(RID^{'}, J_u^{'}, T_{sc}))$ Decryption using shared secret 'P' as symmetric decryption key

ΔT=(T_{uc}-T_{sc})

Check the equivalency of $J_u^{'}$=J_u , if does not hold terminate the session otherwise verify the equivalency of stored RID with the received $RID^{'}$, if does not hold terminate the session, otherwise the legitimacy of the server is achieved. After the mutual authentication user and server both compute the session key as follows: S_k=$h(P||T_{uc}||T_{sc})$

Cell phone first verifies that ΔT is within the permissible range, then checks the equivalency of received $J_u^{'}$ with the computed one at its end. If ΔT is not within the permissible range or $J_u^{'}$ does not match, cell phone application terminates the current session or otherwise server identity is verified along with message freshness . After verifying the server identity, user computes the session key S_k for current session. Server also computes the session key S_k at its end. Our authentication scheme does not only successfully achieves the mutual authentication but it also verifies the legitimacy of the user device. For the verification of the user device, server sends a verification code 'K' to the registered number 'N' of the user. On receiving the verification code 'K' from server, user retrieves 'R' by computing $R = K \oplus RPWD$, retrieves the device's serial number Ser, computes $S_{pub}(R||Ser||T_{uc})$ and sends it to the server. After receiving the input from user, the server decrypts the message using its private key S_{pri} and verifies the 'R' and the received serial number with with the stored ones. On successful verification of both, the server grants the access to the TMIS.

7.7.4 Password Update Phase

In this phase, the user updates his/ her password, the password should be changed and updated at both ends in an efficient manner. The password change should be properly communicated to the server before updating at the user end. Consider a scenario in which user changes his/ her password and fails to communicate the update to the server due to the loss/ unavailability of the communication channel. In such a situation, the user and server will have a different password, hence he/ she will not be able to login to the server and will face denial of service.

Our proposed password update mechanism updates the user password at the user end after getting approval from the server. In password update phase, the user first logs in to the server and requests to initiate the password change mechanism. The password update wizard will ask the user to provide a new password $PWD^{'}$, on receiving the input from the user the wizard computes $RPWD^{'}$=$h(r^{'}||PWD^{'})$, where '$r^{'}$' is a new random nonce. The update wizard computes $S_{pub}(RPWD^{'}, T_{uc})$, where T_{uc} is the current timestamp of the user and S_{pub} is the public key of the server. Cell phone transmits this computed information to the server:

- $U \rightarrow S$ = $S_{pub}(RPWD^{'}, T_{uc})$

On receiving the above information from the user, the server decrypts the received information using its private key S_{pri} and extracts the updated password $RPWD^{'}$ of the user hashed with a new random nonce '$r^{'}$' and the user timestamp. At first, the server verifies the ΔT =(T_{sc}-T_{uc}), where T_{sc} is the current timestamp at the server end, ΔT should be in the permissible range to thwart any replay attack. Server then generates a new random nonce '$R^{'}$' and compute $K^{'}$ =R$^{'}$ $\oplus RPWD$ and sends the verification code '$K^{'}$' to the user's registered cell phone number through GSM channel, On receiving the verification code '$K^{'}$' the application retrieves '$R^{'}$' by computing

$R^{'} = K^{'} \oplus RPWD$. The application also retrieves the serial number Ser of the device, then computes $S_{pub}(R^{'}||Ser||T_{uc})$ and sends it to the server. Server decrypts $S_{pri}(S_{pub}(R^{'}||Ser||T_{uc}))$ the response message from the user. The user then verifies the ΔT =(T_{sc}-T_{uc}), serial number Ser of the device and random nonce '$R^{'}$'. On successful verification, the server computes the following and sends to the user:

$S_{pri}(S_{pub}(RPWD^{'}, T_{uc}))$

$P^{'} = h(R^{'}||ID)$

$Q^{'}$=$P^{'} \oplus RPWD^{'}$

$Y^{'}$=$h(P^{'}||RPWD^{'}||ID)$

- $S \rightarrow U$ = $S_{pri}(Q^{'}, Y^{'}, T_{sc})$

On receiving the information from the server, the cell phone first decrypts the message by using the server's public key S_{pub}, then verifies the ΔT =(T_{uc}-T_{sc}). The successful decryption using server's public key S_{pub} verifies the authenticity of the message that it came from the server and cannot come from anywhere else. After verifying the authenticity of the server, the user computes $Z^{'}$=$h(ID||PWD^{'}) \oplus r$ and saves the new computed values of $Q^{'}$, $Y^{'}$ and $Z^{'}$ and discards the previous computed ones.

In password update phase, the service provider application installed in cell phone computes a new random 'r' that is very critical in computing the shared secret 'P', therefore frequent update of user password becomes very important.Therefore, in proposed model, the server will force the user to update his/her password after every 30 days or after every 50 successful authentication requests, whichever comes first. This will be very helpful in mitigating online password guessing attack, offline guessing attack, replay attack and will also protect user anonymity against attacks on user identity.

The complete flow of the proposed two-factor authentication scheme is presented in Table 7.6 and the notations used in the scheme are given in Table 7.5 for better understanding.

Table 7.5: Description of used notations in proposed schemes

Notation	Description
ID	User chosen identification/ username
PWD	User chosen password
N	Cell phone number of the user
Ser	Serial number of the user device
$RPWD$	Hash of user password after concatenated with 'r' for insider attack protection
R	Random nonce generated at server end
r	Random nonce generated at user end
P	Shared secret
RID	Encrypted user ID after concatenated with 'R', securing user ID for anonymity
Y	Cell phone matches to verify the user ID and PWD during login phase
S_{pri}	Server's private key
S_{pub}	Server's public key
S_k	Session key
E_p	Encryption function using shared secret P as encryption key
D_p	Decryption function using shared secret P as decryption key
K	Verification code sent through GSM
T_{uc}	Current time at user end
T_{uc}	Current time at server end
ΔT	Permissible time after which the message will expire

Table 7.6: Proposed two-factor authentication scheme

Phase	User	TMIS
Registration	'ID', 'PWD'	
	$RPWD = h(r\|\|PWD)$	
	$S_{pub}(ID, N, RPWD, T_{uc})$	
	$\text{U} \xrightarrow{S_{pub}(ID, N, RPWD, T_{uc})} S$	
		$S_{pri}(S_{pub}(ID, N, RPWD, T_{uc}))$
		$T = (T_{sc} - T_{uc})$
		$P = h(R\|\|ID)$
		$Q = P \oplus RPWD$
		$Y = h(P\|\|RPWD\|\|ID)$
		$RID = S_{pub}(ID\|\|R)$
		$K = R \oplus RWPD$
		$\text{U} \xleftarrow{\text{Verification Code '}K\text{' Through GSM}} S$
	$R = K \oplus RWPD$	
	Retrieves serial number	
	'Ser' of the device	
	$S_{pub}(R\|\|Ser\|\|T_{uc})$	
	$\text{U} \xrightarrow{S_{pub}(R\|\|Ser\|\|T_{uc})} S$	
		$S_{pri}(S_{pub}(R\|\|Ser\|\|T_{uc}))$
		ΔT =(T_{sc}-T_{uc})
		Verify the random none 'R'
		$\text{U} \xleftarrow{S_{pri}(Q, RID, Y, T_{sc})} S$
	$S_{pub}(S_{pri}(Q, RID, Y, T_{sc}))$	
	ΔT =(T_{uc}-T_{sc})	
	$Z = h(ID\|\|PWD) \oplus r$	
Login and Authentication	'ID', 'PWD'	
	r=$Z \oplus h(ID\|\|PWD)$	
	$RPWD = h(r\|\|PWD)$	
	$P = Q \oplus RPWD$	
	$Y = h(P\|\|RPWD\|\|ID)$	

Table 7.6: Proposed two-factor authentication scheme

Phase	User	TMIS
	$J_u = h(T_{uc}\|\|P)$	
	$S_{pub}(RID, J_u, T_{uc})$	
	U $\xrightarrow{S_{pub}(RID, J_u, T_{uc})}$ S	
		$S_{pri}(S_{pub}(RID, J_u, T_{uc}))$
		$\Delta T = (T_{sc} - T_{uc})$
		Check if
		$S_{pri}(S_{pub}(ID\|\|R))$
		$P = h(R\|\|ID)$
		$J_u^{'}$=h$(T_{uc}\|\|P)$
		Check if
		$J_u^{'}$=J_u
		$RID^{'}$= $S_{pri}](ID\|\|R)$
		J_s=$E_p(RID^{'}, J_u^{'}, T_{cs})$
		U $\xleftarrow{(J_s, T_{cs})}$ S
	$D_p(E_p(RID^{'}, J_u^{'}, T_{sc}))$	
	ΔT =(T_{uc}-T_{sc})	
	Check if	
	$J_u^{'}$=J_u	
	Check if	
	RID=$RID^{'}$	
	$S_k = h(P\|\|T_{uc}\|\|T_{sc})$	$S_k = h(P\|\|T_{uc}\|\|T_{sc})$
Password Update	$RPWD^{'}$=$h(r^{'}\|\|PWD^{'})$	
	$S_{pub}(RPWD^{'}, T_{uc})$	
	U $\xrightarrow{S_{pub}(RPWD^{'}, T_{uc})}$ S	
		$S_{pri}(S_{pub}(RPWD^{'}, T_{uc}))$
		ΔT=(T_{sc}-T_{uc})
		$K^{'} = R^{'} \oplus RWPD$
		U $\xleftarrow{\text{Verification Code '}K^{'}\text{' Through GSM}}$ S
	$R^{'} = K^{'} \oplus RWPD$	

Table 7.6: Proposed two-factor authentication scheme

Phase	User	TMIS
	Retrieves serial number	
	'Ser' of the device	
	$S_{pub}(R^{'}\|\|Ser\|\|T_{uc})$	
	U $\xrightarrow{S_{pub}(R^{'}\|\|Ser\|\|T_{uc})}$ S	
		$S_{pri}(S_{pub}(R^{'}\|\|Ser\|\|T_{uc}))$
		ΔT=(T_{sc}-T_{uc})
		Verify Random nonce '$R^{'}$' and
		serial number 'Ser' of the device
		$P^{'} = h(R^{'}\|\|ID)$
		$Q^{'}$=$P^{'} \oplus RPWD^{'}$
		$Y^{'}$=$h(P^{'}\|\|RPWD^{'}\|\|ID)$
		U $\xleftarrow{S_{pri}(Q^{'}, Y^{'}, T_{sc})}$ S
	$S_{pub}(S_{pri}(Q^{'}, Y^{'}, T_{sc})$	
	ΔT=(T_{uc}-T_{sc})	
	$Z^{'}$=$h(ID\|\|PWD^{'}) \oplus r$	

7.7.5 Revocation Phase

Users only go through from this phase when they want to revoke their registration due to registered device loss/stolen, 'ID' compromise or password compromise. For an efficient revocation mechanism, user must provide his/her backup cell phone number or email address which he/she can access at an appropriate time accordingly. The backup cell phone number or email address must be provided by the user when he/she login for the first time, the application will not offer its services until backup cell phone number or email address is provided. Incase of device loss, the user downloads the application on any device and goes to the revocation section, this section asks the username, password and registered cell phone number of the user and encrypts them with the

server's public key S_{pub} and sends it to the server. Server upon receiving the message from user, decrypts the message using its private key S_{pri}. Server verifies the 'ID', password and cell phone number, after successful verification, the server demands the backup cell phone number or email address previously provided by the user so that a verification code can be sent to the user. On providing the valid backup cell phone number or email address, the server sends the verification code to the provided input. On receiving the verification code user encrypts the verification code with server's public key S_{pub} and sends it to the server, server upon receiving the message from user decrypts the message using its private key S_{pri}. Server verifies the verification code by matching it with the sent one and on successful verification revokes/terminates the user account so that it cannot be misused by anyone. All the messages sent to user or server contain timestamp so that the freshness of every message can be guaranteed.

7.8 ΔT Criteria

All message transactions between server and user during the authentication process contain ΔT for message freshness validation. ΔT is the maximum permissible life-time of any authentication message in transit, after which the message will expire and will not be considered for any legitimate authentication request. The expired message receiving party will initiate the retransmission request to the sending party so that the authentication request can be further processed.

ΔT is set for 30 seconds for all messages transmitted through Internet and 90 seconds for all messages transmitted through GSM channel. Only three requests for retransmissions are allowed during the authentication process, after which the session will be rejected by both parties.

The criteria can also be made flexible in such a way that the ΔT, the life-time of a message can be increased at geographical locations where Internet bandwidth is thin and speed of communication

is slower than usual, so that users do not face denial of service at remote areas due to bandwidth issues. Similarly, the number of retransmission requests can be made flexible such that it can be increased at remote locations where communication is slower than usual and can also be decreased where communication is more faster and reliable than usual.

7.9 Emergency Handling Mechanism

Emergency situations must be accounted for while designing the security mechanism for accessing the TMIS. In an emergency, the physician should be able to easily access the TMIS on the behalf of the patient so that treatment can be started timely and accordingly. The emergency mechanism should also not so weak that it can be accessed or compromised by an adversary in healthy conditions. So, there is a tradeoff between designing a strong security mechanism and designing a mechanism that can be easily accessed or bypassed. Emergency mechanism should be designed such that it can be activated by the patient himself/herself or by the service provider's trusted staff at the time of emergency on patient's behalf.

We propose an emergency option at the home screen of e-healthcare provider cell phone application. When patient chooses this option, application asks for the registered cell phone number/email for patient identification and verification. The emergency request is authenticated by sending a verification code to the registered cell phone number/email.

There can be a scenario, where patient reaches to hospital/physician in unconscious condition. Physician requires access to the PHI of the patient for his investigation about the condition of the patient. In this scenario, user cannot be asked for the registered cell phone number/email address. The authentication mechanism requires bypassing, so that access to critical information can be acquired in time.

In our proposed model physicians have a strict registration criteria, physician's registration request only approved by the service provider after his/her physical verification on duty by the e-Healthcare provider. So, a physician is also a more trusted user of the e-Healthcare service provider. In emergency conditions, where user cannot be asked for the registered cell phone number/email, physician can use his/her registered cell phone number/email on the patient's device for getting access to patient's PHI. The server approves the access request after verifying the identity of the physician. The server sends the verification code to the physicians registered cell phone number. The event will be recorded in the e-Healthcare service provider database and the alarm notification will also be sent to the user's registered cell phone number/email address irrespective of the fate of the request i.e approved or denied.

The authentication mechanism can also be bypassed or temporarily deactivated by the service provider's trusted staff, who have administrative access to the service provider's database. This temporary deactivation sends the alarm notification to patient as well as to his/her physician. The authentication mechanism will remain deactivated until the patient recovers and leaves the hospital.

The application emergency mechanism can be accessed at any stage or condition (locked) of the cell phone, for this the application must have permissions such that it can be accessed even when the phone is locked, this enables the physician to access the patients PHI by using his/her credentials as he/she does not know the unlock key of the cell phone. It is also necessary because it only enables physician to access the patients PHI not patients personal data which is stored in the cell phone and also prohibited for the physician.

7.10 Conclusion

Chapter 7 covered comparison of authentication categories, proposed hybrid model for authentication, three-factor and two-factor authentication schemes and emergency handling mechanism. From the comparison of authentication categories, it is concluded that three-factor authentication scheme is more secure as compared to two-factor and one-factor authentication schemes. Three-factor authentication scheme provide more security at the cost of more delay, computation cost, communication cost and user easiness. It is also learned that the users are now more comfortable with biometric enabled three-factor authentication schemes, therefore number of devices with biometric feature has increased at an alarming rate recently.

The proposed hybrid model presents separate authentication mechanism for users on the basis of their role in the e-Healthcare architecture. Therefore, for patients, two-factor authentication scheme have been proposed, whereas for physicians three-factor authentication scheme have been proposed in this Chapter 7.

Finally, at the end of the Chapter 7, an emergency handling mechanism have been proposed. The emergency mechanism will help the e-Healthcare provider staff to bypass the authentication mechanism in emergency situations.

Chapter 8

SECURITY ANALYSIS OF PROPOSED SCHEMES

8.1 Introduction

Chapter 8 is divided in four sections. First Section 8.1 contains the introduction of the chapter, second contains the security analysis of the proposed authentication schemes against the online password guessing attack, offline password guessing attack, user impersonation attack, denial-of-service attack, session key disclosure attack, stolen verifier attack and privileged insider attack. Third section presents the computation cost of the proposed schemes, the computation cost of the user and the server have been evaluated separately. Finally, Section four summarizes the Chapter 8 and also presents its conclusion.

8.2 Security Analysis of Proposed Authentication schemes

This section presents the security analysis of proposed schemes (three-factor authentication, two-factor authentication) in the light of proposed performance metrics presented in Chapter 3. The security analysis of the proposed authentication schemes is as follows:

8.2.1 Online Password Guessing Attack

The proposed scheme resists online password guessing attack, as the attacker cannot guess the user password in the absence of random nonce 'r'. The cell phone application does not store the user password in plain, instead it stores in the form of $RPWD = h(r||PWD)$. The attacker cannot get the password even he/she gets the physical access to the user's phone, because it

requires random nonce 'r' to compute the $RPWD = h(r||PWD)$, which in not stored in plane by the application instead it is stored in the form of $Z = h(ID||PWD) \oplus r$. Therefore, the attacker cannot guess the 'ID' and password of the user by mounting online password guessing attack. To retrieve 'r', the attacker must provide the 'ID' and password to compute $r = Z \oplus h(ID||PWD)$ which he/she obviously does not know that is why he/she requires the random nonce 'r'.

8.2.2 Offline Password Guessing Attack

The proposed scheme resists offline password guessing attack, as the attacker cannot retrieve the shared secret 'P' and random nonce 'r' from the application as they are not stored in plain, instead stored as $Q = P \oplus RPWD$, $Y = h(P||RPWD||ID)$ and $Z = h(ID||PWD) \oplus r$. Incase, attacker gets the physical access to the cell phone application and retrieves the stored parameters i.e Q, Y, Z even then he/she would not be able to retrieve the the shared secret 'P' and random nonce 'r' because of the involvement of server generated random nonce R in the shared secret $P = h(R||ID)$. The only way to retrieve the shared secret from $Q = P \oplus RPWD$ is to retrieve the random nonce 'r' first, so that $RPWD = h(r||PWD)$ can be calculated. The only parameter stored in cell phone containing 'r' is $Z = h(ID||PWD) \oplus r$, to retrieve 'r' from $Z = h(ID||PWD) \oplus r$ attacker must know the 'ID' and 'PWD', therefore we can verify that attacker cannot retrieve 'r' as all three parameter in $Z = h(ID||PWD) \oplus r$ are unknown to the attacker.

8.2.3 User Impersonation Attack

The proposed scheme resists the user impersonation attack, as the attacker cannot compute the valid login request containing $J_u = h(T_{uc}||P)$ without the knowledge of the shared secret 'P'. Beside, before sending the login request to the server, the cell phone application authenticates

the user at its end. To be authenticated by the cell phone, the attacker must guess the 'ID' and password 'PWD' pair simultaneously, which is not possible in polynomial time. In addition, each valid login request contain timestamp, which makes the impersonation attack by the attacker by replaying the login request also makes it impossible, therefore the attacker cannot impersonate as a valid user.

8.2.4 Denial-of-Service Attack

The proposed scheme resists the denial-of-service attack, as the cell phone application does not send the login request to the server until it authenticates at its end. In the login phase, user keys his 'ID' and password, the cell phone application retrieves $r = Z \oplus h(ID||PWD)$ and computes $RPWD = h(r||PWD)$, $P = Q \oplus RPWD$ and $Y = h(P||RPWD||ID)$ and matches it with the stored 'Y', if it matches the application forwards the the login request to the server, otherwise it terminates the login session at its end. Therefore, the attacker cannot mount denial-of-service attack without being authenticated at the cell phone end first.

8.2.5 Session Key Disclosure

The proposed scheme resists the denial-of-service attack, as session key cannot be computed by the adversary. The session key is computed using the shared secret $S_k = h(P||T_{uc}||T_{sc})$, the shared secret is computed using the server generated random number 'R' which is only known to server, therefore session key cannot be computed by the attacker.

8.2.6 Stolen Verifier Attack

The proposed scheme resists the stolen verifier attack, as attacker cannot obtain user identity from server's database. The server does not store user 'ID' in plain, instead it stores the 'ID' in the

form of $P = h(R||ID)$, therefore without the knowledge of server generated random nonce 'R' an attacker cannot obtain the user 'ID'.

8.2.7 Privileged Insider Attack

The proposed scheme resists the privileged insider attack, as attacker cannot obtain user password 'PWD' from server's database. User does not provide his/her password in plain to the server, instead password is provided in the form of $RPWD = h(r||PWD)$. The insider cannot obtain the password without the knowledge of the user generated random nonce 'r', which was never sent to the server, therefore, any privileged insider cannot retrieve password from server's database.

8.2.8 Ensures User Anonymity

The proposed scheme ensures user anonymity, as the cell phone application does not store the user 'ID' in plain, instead, the user 'ID' is stored in the form of $Z = h(ID||PWD) \oplus r$, $Q = P \oplus RPWD$, $Y = h(P||RPWD||ID)$ and $RID = S_{pub}(ID||R)$. During the registration phase, the user 'ID' does not travel on the communication channel in plain, instead, the cell phone application encrypts it with the server's S_{pub}, $S_{pub}(ID, N, RPWD, F_i, T_{uc})$ before its transmission on the public channel. The attacker cannot retrieve the user 'ID' from $RID = S_{pub}(ID||R)$ without the knowledge of server's private key S_{pri}. During the login and authentication phase, the user 'ID' also does not send the 'ID' on communication channel in plain, instead, it travels in the form of $RID = S_{pub}(ID||R)$ and J_s=E_p($RID^{'}$, $J_u^{'}$, T_{sc}), therefore an attacker cannot retrieve the user 'ID' from $RID = S_{pub}(ID||R)$ without the knowledge of server's private key S_{pri} and similarly cannot retrieve it from J_s=E_p($RID^{'}$, $J_u^{'}$, T_{sc}) without the knowledge of the shared secret 'P'.

8.2.9 Initial Authentication at Cell Phone

The proposed scheme authenticates the user at the user end first, before sending any login request to the server to guard against DOS attacks. It sends the login request to the server only after the successful authentication at the user end. The application computes the $RPWD = h(r||PWD)$ and $Y = h(P||RPWD||ID)$ from the received 'ID' and password 'PWD' provided by the user and matches the stored 'Y' with the computed one, the successful match verifies that the user is the valid user of the application, otherwise the session is rejected. The cell phone application does not send any authentication request to the server, until the computed 'Y' matches with the stored one. Hence, the cell phone authenticates the user at the user end before sending any authentication request to the server.

8.2.10 Mutual authentication

The proposed scheme ensures mutual authentication and resists user impersonation attack as well as server impersonation attacks. The server computes $J_u^{'} = h(T_{uc}||P)$ and matches it with the received one 'J_u' from the user, the successful match ensures the legitimacy of the user, because no one else can have the shared secret 'P'. Similarly, the user matches 'RID' with the received one from the server '$RID^{'}$', the equivalency verifies the legitimacy of the server, because no one else can have the shared secret 'P' to compute J_s=$E_p(RID^{'}, J_u^{'}, T_{sc})$. Hence, the scheme achieves mutual authentication using the shared secret 'P'.

8.3 Computation Cost

This Section 8.3 presents the computation cost of the proposed scheme. The proposed scheme is designed such that the computation cost remains within the low or in the medium category for all of the phases of the authentication scheme. The computation cost of the login and authentication

phase is more important than the registration phase, which occurs only once while the login and authentication phase occurs whenever user attempts to access the TMIS. The computation cost of the login and authentication phase is computed by calculating the number of operations performed during these phases. The computation cost of user and server during the registration, login and authentication phase are presented as follows.

8.3.1 User Computations

The user computation cost is computed by calculating the number of function operations performed by the user during the login and authentication phase. During the login and authentication phase, hash function calculations have have been performed eight times, encryption and decryption function operations have been performed six times while ignoring XOR operations as they do not take considerable time for computation. Among eight hash operations, six operations have been performed by the user. Similarly, among six encryption/ decryption operations, two operations have been performed at the user end. In total, user have performed eight operations, which falls under the medium category described in Chapter 5 and also presented in [92]. In three-factor authentication scheme, the user performs an additional computation i.e the bio-hash function for the verification of the user biometric information. We ignored the XOR operations as XOR are one step operations and take very less time to compute as compared to hash and encryption/ decryption operations.

8.3.2 Server Computations

The server computation cost is computed by calculating the number of operations performed at the server end during the login and authentication phase. In the login and authentication phase, hash function calculations have have been performed eight times, encryption and decryption func-

tion operations have also been performed six times while ignoring the XOR operations as they do not take considerable time for computation. Among eight hash operations, only two hash operations have been performed by the server. Similarly, among six encryption/ decryption function operations, four such operations have been performed at the server end. In total, the server has performed six operations which falls under the medium category of computation cost described in Chapter 5 and also presented in [92].

The computation cost of the the user and the server for the proposed three-factor and two-factor authentication schemes is presented in Table 8.1, similarly the security index of the proposed authentication schemes is presented in Table 8.2, the table is tabulated on the basis of security and privacy properties mentioned in Chapter 2, Section 2.3 and listed as follows:

A1: Ensure user anonymity

A2: Resist insider attack

A3: Ensure efficient password update

A4: Ensure session key verification

A5: Ensure forward secrecy

A6: Resist denial of service attack

A7: Resist off-line password guessing attack

A8: Resist stolen smart card/ phone attack

A9: Resist user impersonation attack

A10: Resist stolen verifier attack

A11: Resist replay attack

SI: Security index

Table 8.1: Computation cost of proposed schemes

Phase	User Computations	Server Computations
	Three-Factor Authentication Scheme	
Registration	$1T_H + 2T_h + 3T_s$+$1T_{xor}$	$2T_h + 3T_s$+$1T_{xor}$
Login and Authentication	$1T_H + 5T_h + 2T_s$+$2T_{xor}$	$2T_h + 4T_s$
Password Update	$2T_h + 3T_s$+$1T_{xor}$	$2T_h + 2T_s$+$1T_{xor}$
	Two-Factor Authentication Scheme	
Registration	$2T_h + 3T_s + 1T_{xor}$	$2T_h + 3T_s$+$1T_{xor}$
Login and Authentication	$5T_h + 2T_s + 2T_{xor}$	$2T_h + 4T_s$
Password Update	$2T_h + 3T_s$+$1T_{xor}$	$2T_h + 2T_s$+$1T_{xor}$

Table 8.2: Security and privacy properties of proposed schemes

Scheme	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	SI
Proposed Schemes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	11

8.4 Conclusion

This Chapter 8 presented the security and computation cost analysis of the proposed three-factor and two-factor authentication schemes. From the security analysis of the proposed authentication scheme, it is concluded that the proposed schemes resists offline password guessing attack, online password guessing attack, user impersonation attack, denial-of-service attack, session key disclosure attack, stolen verifier attack, privileged insider attack and ensures user anonymity, mutual authentication and initial authentication at cell phone end. The security index of the proposed scheme presented in Table 8.2 is the highest among all the evaluated authentication schemes pre-

sented in Chapter 4, 5 and 6.

From the computation cost analysis presented in Table 8.1, it can be observed that the computation cost of both, the user and the server falls under the medium category [92], while ensuring all the security and privacy properties. There is no other evaluated scheme in Chapter 4, 5 and 6, that achieves higher security index while keeping the computation cost at medium category or lower.

Chapter 9

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

9.1 Introduction

Chapter 9 is divided in three sections. First Section 9.1 contains the introduction of the chapter, Second Section 9.2 contains the conclusion of the research work based on the literature review and proposed solution, and finally third Section 9.3 contains the future research directions.

9.2 Conclusion

In this research we have analyzed security and privacy properties, user efficiency, server efficiency, as well as advantages and disadvantages of one-factor, two-factor and three-factor authentication schemes. We have also analyzed the tradeoff between ensured security and mobility. The one-factor authentication schemes have the least delay and are the most user friendly but they do not provide adequate security. Two-factor authentication schemes tend to ensure desired security at the cost of more delay and user interaction. Three-factor authentication schemes provide equivalent security to two-factor authentication schemes at the cost of more delay and user interaction but they also add another layer of security that ensures increased hard work for the adversary. As two-factor and three-factor authentication schemes provide equivalent security, both can be used for authentication in e-Healthcare infrastructure. Two-factor authentication schemes for the ordinary users and three-factor authentication schemes for the physicians are suggested, as physicians have the elevated access to the TMIS. Similarly, smart devices are suggested for all the users as

the second layer of security to reap the benefits of mobility. A hybrid solution is recommended that offers two-factor authentication methods to patients and three-factor authentication methods to physicians.

The reviewed schemes in our literature review lack the practical approach, as most of them require a secure channel for registration phase. The proposed schemes do not differentiate between the physicians and the user, while clearly there is a big difference between their roles and their privileges. The researchers who proposed three-factor authentication schemes did not cater the fact that not all users of cell phones have a biometric sensor embedded in their cell phone. Similarly, the researchers who proposed two-factor authentication scheme did not take the advantage of the third factor for the physicians.

Other proposed schemes lack in addressing emergency situations. The designed authentication mechanism should be such that, it can be easily bypassed at the time of emergency by the user or the by the physician. Similarly, the reviewed schemes do not verify the biometric information at both ends i.e. the user end and the server end. As mobile apps can be manipulated, it is necessary to verify the biometric information at server end as well. Our proposed scheme verify the biometric information at both ends to thwart any attack that can be launched by manipulating biometric information at the user end. To minimize the delay and computation cost, several schemes do not authenticate the user at the user end first, which can increase the communication cost incase user enters the wrong credentials by mistake. This also allows adversary to launch denial-of-service attack by exhausting the resources of the server with false authentication requests in bulk. Our proposed authentication scheme authenticates the user at the user end first before sending any authentication requests to the server.

From the security analysis of our proposed authentication schemes it is established that our

schemes resist offline password guessing attack, online password guessing attack, user impersonation attack, denial-of-service attack, session key disclosure attack, stolen verifier attack, privileged insider attack and ensures user anonymity, mutual authentication and initial authentication at cell phone end. The computation cost is also reasonable for practical implementation.

The security index of our proposed schemes presented in Table 8.2 is the highest among all the evaluated authentication schemes presented in Chapter 4, 5 and 6. Similarly, from the computation cost analysis presented in Table 8.1, it can be observed that the computation cost of both, the user and the server falls under the medium category [92], while ensuring all the security and privacy properties. There is no other evaluated scheme in Chapter 4, 5 and 6, that achieves higher security index while keeping the computation cost at medium category or lower.

Our proposed scheme also, verifies the device from which user tries to access the TMIS. $RID = S_{pk}(ID||R)$ is sent to the user by the server in the registration phase. User sends this received 'RID' to the server in the login phase, the server matches this with the one it sent to the user in the registration phase. The match implies that the user is sending the login request from the same device, which he/she used for the registration phase. As a valid 'RID' requires server's private key S_{pk}, which is only known to the server, so an adversary cannot generate a valid 'RID'. The device is dully verified by sending a verification code 'K', when a physician tries to access the TMIS, as he/she has the elevated access which requires more strengthened security.

In the proposed scheme, every information is verified at the user end before sending it to the server. Any session initiated by the adversary is terminated at the user end before consuming any bandwidth, as any information provided by the logging user is first verified at the user end. This feature also protects the TMIS for denial-of-service attacks from the adversary. The computation and communication cost is reasonable for practical implementation of the proposed schemes as

presented in 8.1.

For practical implementation of any authentication method/ scheme for e-Healthcare, local and international laws must be observed. These laws address the user's privacy and security concerns, some of them are:

- *Health Insurance Portability and Accountability Act (HIPAA):* This law protects user's confidentiality and privacy. The law forbids anyone to use patient's health record for any purpose without patient's consent.
- *Health Information Technology for Economic and Clinical Health (HITECH):* This law addresses user's privacy and security concerns associated with the electronic transmission of health records. It ensures that patient's health records are encrypted and bound the physicians to destroy unencrypted health records after use.
- *Personal Health Information Protection Act (PHIPA):* This law establishes some rules for collection, use and disclosure of patient's health records. It addresses confidentiality and privacy concerns of the users.

There are also some standards like: ISO 27799:2016 and ISO/IEC 17799, which provide guidelines and best practices for e-Healthcare. One-factor authentication methods fail to fulfill the minimum requirements set by these laws to ensure users privacy, whereas two-factor authentication methods can comply with the minimum requirements of these laws. It is also noticed that this category of authentication schemes is currently recommended in e-Health industry [158, 159, 160, 161]. Although, three-factor authentication methods fulfill the above mentioned requirements but current e-Health infrastructure does not fully support these methods.

9.3 Future Research Directions

As e-Healthcare is a new service delivery mechanism in the field of healthcare services, it has comparatively vast scope for contribution than other established fields. Contribution of our research work in the field of e-Healthcare is described as follows:

1. We have designed a performance criteria for authentication schemes, the criteria serves as a guideline for the researchers in designing their authentication schemes for the e-Healthcare.
2. We have evaluated several well-known authentication schemes against the proposed performance matrix and ranked them accordingly, which provides a holistic view of the existing authentication schemes and also highlights the areas of improvement in those authentication schemes.
3. We have evaluated and highlighted the advantages and disadvantages of different authentication categories, which helps the researchers choosing a category for designing their authentication schemes.
4. We have proposed a role based novel solution, that takes the benefits of all categories to meet the user expectations from the e-Healthcare services.
5. We have proposed two different authentication schemes, one for the patients and the other for the physicians. The security analysis proves that the proposed schemes meet and satisfy the proposed performance criteria designed for the evaluation of authentication schemes.

As future research work, the proposed scheme can be simulated using different authentication verification tools. The simulation results will further enhance the credibility and correctness of the proposed schemes. The proposed scheme can be developed and integrated on any mobile platform for practical usage purpose. As future research direction, the risk mechanism can be introduced in the proposed schemes. A risk profile based on the registered user and the device

behavior can be generated, the generated risk profile will be consulted whenever any user will try to access the TMIS. The risk profile can include device's GPS location, MAC address, serial number, IP address, user login time etc. In high risk scenario, the server will have to verify the legitimacy of the access request by sending a verification code to the patients/ physicians device and/ or by asking security questions.

BIBLIOGRAPHY

[1] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients data privacy using wireless body area networks," Procedia Computer Science **34,** 511–517 (2014).

[2] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "Security and Privacy for Mobile Healthcare (m-Health) Systems,", 2011.

[3] T. Adamsk and W. Winieck, "Entity identification algorithms for distributed measurement and control systems with asymmetry of computational power," PRZEGLAD ELEKTROTECHNICZNY **84,** 216–219 (2008).

[4] X. Cheng and M. Li, "The authentication of the grid monitoring system for wireless sensor networks," Prz Elektrotechniczn (2013).

[5] J. Pejaś, I. El Fray, and A. Ruciński, "Authentication protocol for software and hardware components in distributed electronic signature creation system," Prz Elektrotechniczn (2012).

[6] L. Lamport, "Password authentication with insecure communication," Communications of the ACM **24,** 770–772 (1981).

[7] T. Hwang, Y. Chen, and C. S. Laih, "Non-interactive password authentications without password tables," In *Computer and Communication Systems, 1990. IEEE TENCON'90., 1990 IEEE Region 10 Conference on*, pp. 429–431 (1990).

[8] Y. Zhang, D. Zhang, M. M. Hassan, A. Alamri, and L. Peng, "CADRE: Cloud-assisted

drug recommendation service for online pharmacies," Mobile Networks and Applications **20,** 348–355 (2015).

[9] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Electronics **50,** 231–235 (2004).

[10] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," Journal of medical systems **40,** 1–15 (2016).

[11] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," Version v0 **31,** 15 (2008).

[12] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," (2010).

[13] Y.-M. Tseng, "Weakness in simple authenticated key agreement protocol," Electronics Letters **36,** 1 (2000).

[14] R. Amin and G. Biswas, "An improved rsa based user authentication and session key agreement protocol usable in tmis," Journal of Medical Systems **39,** 1–14 (2015).

[15] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," IEEE Transactions on Consumer Electronics **49,** 1246–1248 (2003).

[16] R.-J. Hwang, C.-H. Lai, and F.-F. Su, "An efficient signcryption scheme with forward secrecy based on elliptic curve," Applied Mathematics and computation **167,** 870–881 (2005).

[17] D. Adrian *et al.*, "Imperfect forward secrecy: How Diffie-Hellman fails in practice," In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 5–17 (2015).

[18] J. Jau, "Password update systems and methods,", 2005, uS Patent App. 11/289,029.

[19] S. H. Islam and G. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," Mathematical and Computer Modelling **57,** 2703–2717 (2013).

[20] X.-l. Li, Q.-y. Wen, H. Zhang, Z.-p. Jin, and W.-m. Li, "Offline password guessing attacks on smart-card-based remote user authentication schemes," In *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation*, pp. 81–89 (2016).

[21] S. E. Schechter, D. A. Molnar, J. R. Lorch, B. C. Bond, and B. J. Parno, "Utilization of a protected module to prevent offline dictionary attacks,", 2016, uS Patent App. 15/048,989.

[22] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Transactions on dependable and secure computing **9,** 128–141 (2012).

[23] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics **50,** 629–631 (2004).

[24] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]," In *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*, pp. 187–191 (1994).

[25] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, applica-

tion," IJCEM International Journal of Computational Engineering & Management **11,** 32–37 (2011).

[26] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," International Journal of Computer Applications **9,** 11–15 (2010).

[27] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research," in *Insider Attack and Cyber Security* (Springer, 2008), pp. 69–90.

[28] C. W. Probst, R. R. Hansen, and F. Nielson, "Where can an insider attack?," In *International Workshop on Formal Aspects in Security and Trust*, pp. 127–142 (2006).

[29] S. Jiang, S. Smith, and K. Minami, "Securing web servers against insider attack," In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, pp. 265–276 (2001).

[30] A. Sarkar, S. Köhler, S. Riddle, B. Ludäscher, and M. Bishop, "Insider attack identification and prevention using a declarative approach," In *Security and Privacy Workshops (SPW), 2014 IEEE*, pp. 265–276 (2014).

[31] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," IEEE Internet Computing **10,** 82–89 (2006).

[32] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," In *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*, pp. 208–223 (1997).

[33] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," computer **35,** 54–62 (2002).

[34] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," In *2006 8th International Conference Advanced Communication Technology*, **2,** 6–pp (2006).

[35] R. Latif, H. Abbas, S. Latif, and A. Masood, "EVFDT: an Enhanced Very Fast Decision Tree algorithm for detecting distributed denial of service attack in cloud-assisted wireless body area network," Mob. Inf. Syst pp. 1–13 (2015).

[36] A. Burg, "Ad hoc network specific attacks," In *Seminar Ad hoc networking: Concepts, Applications, and Security. Technische Universitat Munchen,03*, (2003).

[37] T. Tsuji and A. Shimizu, "An impersonation attack on one-time password authentication protocol OSPA," IEICE Transactions on Communications **86,** 2182–2185 (2003).

[38] L. Tamilselvan and D. V. Sankaranarayanan, "Prevention of impersonation attack in wireless mobile ad hoc networks," International Journal of Computer Science and Network Security (IJCSNS) **7,** 118–123 (2007).

[39] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," ETRI journal **32,** 704–712 (2010).

[40] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," Multimedia Tools and Applications **75,** 181–197 (2016).

[41] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," International Journal of Communication Systems **28,** 383–393 (2015).

[42] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers **51,** 541–552 (2002).

[43] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards.," Smartcard **99,** 151–161 (1999).

[44] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," In *Annual International Cryptology Conference*, pp. 398–412 (1999).

[45] T. S. Messerges, *Power analysis attacks and countermeasures for cryptographic algorithms* (University of Illinois at Chicago, 2000).

[46] Y. Li, M. Chen, and J. Wang, "Introduction to side-channel attacks and fault attacks," In *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, **1,** 573–575 (2016).

[47] K. Watanabe, T. Masuda, T. Ohyama, H. Saitoh, Y. Takasaki, and M. Okumura, "Biometric information processing apparatus and biometric information processing method,", 2011, uS Patent 7,899,216.

[48] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE 92, no. 6 (2004): 948-960 **92,** 948–960 (2004).

[49] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern recognition **37,** 2245–2255 (2004).

[50] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," Pattern recognition **40,** 1057–1065 (2007).

[51] L. Leng, A. B. J. Teoh, M. Li, and M. K. Khan, "A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional PalmPhasor-fusion," Security and Communication Networks **7,** 1860–1871 (2014).

[52] L. Leng and A. B. J. Teoh, "Alignment-free row-co-occurrence cancelable palmprint fuzzy vault," Pattern Recognition **48,** 2290–2303 (2015).

[53] L. Nanni and A. Lumini, "Random subspace for an improved biohashing for face authentication," Pattern Recognition Letters **29,** 295–300 (2008).

[54] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM **21,** 120–126 (1978).

[55] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)," In *Fifth International Conference on Communication Systems and Network Technologies (CSNT), 2015*, pp. 776–780 (2015).

[56] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on information theory **29,** 198–208 (1983).

[57] J. Malone-Lee and W. Mao, "Two birds one stone: signcryption using RSA," In *Cryptographers Track at the RSA Conference*, pp. 211–226 (2003).

[58] D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1," In *Annual International Cryptology Conference*, pp. 1–12 (1998).

[59] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation **48,** 203–209 (1987).

[60] V. S. Miller, "Use of elliptic curves in cryptography," In *Advances in Cryptology-CRYPTO85 Proceedings*, pp. 417–426 (1985).

[61] M. Aydos, T. Yantk, and C. Koc, "A high-speed ECC-based wireless authentication on an ARM microprocessor," In *Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference*, pp. 401–409 (2000).

[62] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 119–132 (2004).

[63] K. Gupta and S. Silakari, "Ecc over rsa for asymmetric encryption: A review," IJCSI International Journal of Computer Science Issues 8 (2011).

[64] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, "Comparison of ecc and rsa algorithm in resource constrained devices," In *IT Convergence and Security (ICITCS), 2013 International Conference on*, pp. 1–3 (2013).

[65] M. Savari, M. Montazerolzohour, and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," In *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012*, pp. 49–53 (2012).

[66] T. Y. Woo and S. S. Lam, "A lesson on authentication protocol design," ACM SIGOPS Operating Systems Review **28,** 24–37 (1994).

[67] A. Harbitter and D. A. Menasce, "A methodology for analyzing the performance of authentication protocols," ACM Transactions on Information and System Security (TISSEC) **5,** 458–491 (2002).

[68] K. Thilagavathi and P. Rajeswari, "Efficiency and Effectiveness Analysis over ECC-Based Direct and Indirect Authentication Protocols: An Extensive Comparative Study," ICTACT Journal on Communication Technology **3,** 515–524 (2012).

[69] S. Prasanna and M. Gobi, "PERFORMANCE ANALYSIS OF DISTINCT SECURED AUTHENTICATION PROTOCOLS USED IN THE RESOURCE CONSTRAINED PLATFORM.," ICTACT Journal on Communication Technology 5 (2014).

[70] A. K. Agarwal and W. Wang, "Measuring performance impact of security protocols in wireless local area networks," In *2nd International Conference on Broadband Networks, 2005.*, pp. 581–590 (2005).

[71] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: healthcare cyber-physical system assisted by cloud and big data," (2015).

[72] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," Journal of medical systems **36,** 1529–1535 (2012).

[73] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," Journal of medical systems **36,** 3597–3604 (2012).

[74] Y.-M. Huang, M.-Y. Hsieh, H.-C. Chao, S.-H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," IEEE journal on selected areas in communications **27,** 400–411 (2009).

[75] S. González-Valenzuela, M. Chen, and V. C. Leung, "Mobility support for health monitoring at home using wearable sensors," IEEE Transactions on Information Technology in Biomedicine **15,** 539–549 (2011).

[76] O. Hamdi, M. A. Chalouf, D. Ouattara, and F. Krief, "eHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues," Journal of Network and Computer Applications **46,** 100–112 (2014).

[77] A. Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward energy-efficient and trustworthy eHealth monitoring system," China Communications **12,** 46–65 (2015).

[78] H. Ng, M. Sim, and C. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal **24,** 138–144 (2006).

[79] E. E. Egbogah and A. O. Fapojuwo, "A survey of system architecture requirements for health care-based wireless sensor networks," Sensors **11,** 4875–4898 (2011).

[80] H. Jemal, Z. Kechaou, M. B. Ayed, and A. M. Alimi, "Mobile Cloud Computing in Healthcare System," in *Computational Collective Intelligence* (Springer, 2015), pp. 408–417.

[81] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," IEEE Access **4,** 1375–1384 (2016).

[82] M. K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," Chaos, Solitons & Fractals **35,** 519–524 (2008).

[83] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," IEEE Wireless Communications **20,** 12–21 (2013).

[84] M. Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," In *DIMACS workshop on usable privacy and security software*, 2010 (2004).

[85] T. R. Kumar and S. Raghavan, "PassPattern System (PPS): a pattern-based user authentication scheme," In *International Conference on Research in Networking*, pp. 162–169 (2008).

[86] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," Computers & Security **30,** 208–220 (2011).

[87] A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM **42,** 40–46 (1999).

[88] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," Computers & Security **28,** 47–62 (2009).

[89] C. Braz and J.-M. Robert, "Security and usability: the case of the user authentication methods," In *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, pp. 199–203 (2006).

[90] L. Koved and B. Zhang, "Improving Usability of Complex Authentication Schemes Via Queue Management and Load Shedding," In *Symposium on Usable Privacy and Security (SOUPS)*, (2014).

[91] Y. Zhang, M. Chen, D. Huang, D. Wu, and Y. Li, "iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization," Future Generation Computer Systems (2016).

[92] M. U. Aslam, A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, and B. Aslam, "A

survey of authentication schemes in telecare medicine information systems," Journal of medical systems **41,** 14 (2017).

[93] Y. Zhang, "GroRec: a group-centric intelligent recommender system integrating social, mobile and big data technologies," IEEE Transactions on Services Computing (2016).

[94] A. Shimizu, "A dynamic password authentication method using a one-way function," Systems and computers in Japan **22,** 32–40 (1991).

[95] L. Harn, "A public-key based dynamic password scheme," In *Symposium on Applied Computing, 1991.,[Proceedings of the 1991]*, pp. 430–435 (1991).

[96] J. G. Steiner, B. C. Neuman, and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems.," In *USENIX Winter*, pp. 191–202 (1988).

[97] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," In *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*, pp. 72–84 (1992).

[98] N. Haller, "The S/KEY one-time password system," (1995).

[99] H. Gwoboa, "Password authentication without using a password table," Information Processing Letters **55,** 247–250 (1995).

[100] C. Chang and T. Wu, "A password authentication scheme without verification tables," In *8th IASTED International Symposium of Applied Informatics. Innsbruck, Austria*, pp. 202–204 (1990).

[101] Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer communications **32,** 583–585 (2009).

[102] C.-K. Chan and L.-M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics **46,** 992–993 (2000).

[103] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," IEEE Transactions on Knowledge and Data Engineering **14,** 445–446 (2002).

[104] C.-C. Lee, M.-S. Hwang, and W.-P. Yang, "A flexible remote user authentication scheme using smart cards," ACM SIGOPS Operating Systems Review **36,** 46–52 (2002).

[105] C.-C. Lee, L.-H. Li, and M.-S. Hwang, "A remote user authentication scheme using hash functions," ACM SIGOPS Operating Systems Review **36,** 23–29 (2002).

[106] J.-J. Shen, C.-W. Lin, and M.-S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics **49,** 414–416 (2003).

[107] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," IEEE Transactions on Consumer Electronics **46,** 958–961 (2000).

[108] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme," Computer Communications **34,** 305–309 (2011).

[109] H.-M. Chen, J.-W. Lo, and C.-K. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems," Journal of medical systems **36,** 3907–3915 (2012).

[110] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A privacy enhanced authentication scheme for telecare medical information systems," Journal of medical systems **37,** 1–8 (2013).

[111] S. Kumari, M. K. Khan, and R. Kumar, "Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems," Journal of medical systems **37,** 1–11 (2013).

[112] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," Journal of Medical Systems **36,** 1989–1995 (2012).

[113] T.-F. Lee, "An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems," Journal of medical systems **37,** 1–9 (2013).

[114] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," Journal of medical systems **36,** 3833–3838 (2012).

[115] A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system," Journal of medical systems **37,** 1–17 (2013).

[116] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems," Journal of Medical Systems **38,** 1–7 (2013).

[117] S. H. Islam and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," Journal of medical systems **38,** 1–16 (2014).

[118] S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, "Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems," Journal of Medical Systems **39,** 1–11 (2015).

[119] L. Zhang, S. Tang, and Z. Cai, "Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card," International Journal of Communication Systems **27,** 2691–2702 (2014).

[120] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems," Journal of medical systems **38,** 1–8 (2014).

[121] D. Mishra, J. Srinivas, and S. Mukhopadhyay, "A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems," Journal of medical systems **38,** 1–10 (2014).

[122] H. Tu, N. Kumar, N. Chilamkurti, and S. Rho, "An improved authentication protocol for session initiation protocol using smart card," Peer-to-Peer Networking and Applications **8,** 903–910 (2014).

[123] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, and M. U. Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP," Peer-to-Peer Networking and Applications pp. 1–15 (2015).

[124] M. S. Farash, "Security analysis and enhancements of an improved authentication for session initiation protocol with provable security," Peer-to-Peer Networking and Applications **9,** 82–91 (2016).

[125] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," Peer-to-Peer Networking and Applications pp. 1–14 (2015).

[126] F. Wen and D. Guo, "An improved anonymous authentication scheme for telecare medical information systems," Journal of medical systems **38,** 1–11 (2014).

[127] F. Wen, "A more secure anonymous user authentication scheme for the integrated EPR information system," Journal of medical systems **38,** 1–7 (2014).

[128] Q. Xie, W. Liu, S. Wang, L. Han, B. Hu, and T. Wu, "Improvement of a uniqueness-and-anonymity-preserving user authentication scheme for connected health care," Journal of medical systems **38,** 1–10 (2014).

[129] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," In *Advances in Cryptology-CRYPTO99*, pp. 388–397 (1999).

[130] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems-CHES 2004* (Springer, 2004), pp. 16–29.

[131] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," In *Cryptographic Hardware and Embedded SystemsCHES 2001*, pp. 251–261 (2001).

[132] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Cryptographic Hardware and Embedded Systems–CHES 2008* (Springer, 2008), pp. 426–442.

[133] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," Journal of Cryptographic Engineering **1,** 5–27 (2011).

[134] F.-X. Standaert, T. G. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology-EUROCRYPT 2009* (Springer, 2009), pp. 443–461.

[135] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," In *Cryptographic Hardware and Embedded Systems*, pp. 144–157 (1999).

[136] D.-R. S. Ya-Fen Chang, Shih-Hui Yu, "A uniqueness-and anonymity- preserving remote user authentication scheme for connected health care," Journal of medical systems pp. 1–09 (2013).

[137] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," Journal of medical systems **37,** 1–16 (2013).

[138] K.-W. Kim and J.-D. Lee, "On the security of two remote user authentication schemes for telecare medical information systems," Journal of medical systems **38,** 1–11 (2014).

[139] F. Wen, "A Robust Uniqueness-and-Anonymity-Preserving Remote User Authentication Scheme for Connected Health Care," Journal of medical systems pp. 1–09 (2013).

[140] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," Journal of medical systems **39,** 1–9 (2015).

[141] R. Amin and G. Biswas, "A secure three-factor user authentication and key agreement protocol for tmis with user anonymity," Journal of medical systems **39,** 1–19 (2015).

[142] A. K. Awasthi and K. Srivastava, "A biometric authentication scheme for telecare medicine information systems with nonce," Journal of medical systems **37,** 1–4 (2013).

[143] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," Journal of medical systems **38,** 1–9 (2014).

[144] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," Journal of medical systems **38,** 1–12 (2014).

[145] X. Yan, P. L. Weiheng Li, J. Wang, and P. G. Xinhong Hao, "A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems," Journal of medical systems **37,** 1–6 (2014).

[146] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," Journal of Medical Systems **39,** 1–8 (2015).

[147] S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, "An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography," Journal of Medical Systems **39,** 1–12 (2015).

[148] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. K. Khan, "Cryptanalysis and improvement of Yan et al.s biometric-based authentication scheme for telecare medicine information systems," Journal of medical systems **38,** 1–12 (2014).

[149] D. Giri, T. Maitra, R. Amin, and P. Srivastava, "An efficient and robust rsa-based remote user authentication for telecare medical information systems," Journal of medical systems **39,** 1–9 (2015).

[150] M. K. Khan and S. Kumari, "An authentication scheme for secure access to healthcare services," Journal of medical systems **37,** 1–12 (2013).

[151] R. Amin and G. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in tmis," Journal of medical systems **39,** 1–17 (2015).

[152] R. Amin and G. Biswas, "Cryptanalysis and design of a three-party authenticated key exchange protocol using smart card," Arabian Journal for Science and Engineering **40,** 3135–3149 (2015).

[153] "Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018,", https://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration, accessed: 2018-3-3.

[154] "Consumers Want Biometric Smartphones, and Love Fingerprint Scanning: FPC Study,", https://findbiometrics.com/consumers-love-fingerprint-scanning-fpc-study-409301//.

[155] "Global Biometric Market Analysis: Trends and Future Prospects,", https://www.bayometric.com/global-biometric-market-analysis/, accessed: 2018-4-8.

[156] "More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018,", https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be accessed: 2018-3-3.

[157] M. Soltane and M. Bakhti, "Multi-modal biometric authentications: concept issues and applications strategies," International Journal of Advanced Science and Technology 48 (2012).

[158] "Does HIPAA require two-factor authentication?,", http://hipaapoliciesandprocedures.com/f-a-q/does-hipaa-require-two-factor-authentication.

[159] "Authentication, Access Control, and Authorization,", https://www.healthit.

gov/facas/FACAS/sites/faca/files/Baker_HITSC_PSWG_revisions.pdf, accessed: 2014-04-24.

[160] "Identity and Access Management for Health Information Exchange,", https://www.healthit.gov/sites/default/files/identitymanagementfinal.pdf, accessed: 2013-12-15.

[161] "State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals,", https://www.healthit.gov/sites/default/files/briefs/oncdatabrief32_two-factor_authent_trends.pdf, accessed: 2015-11-15.

Appendix A

ACRONYMS

TMIS: Telecare Medical information system

PHI: Protected health information

DOS: Denial-of-Service

RSA: River-Shamir-Adleman

ECC: Elliptic curve cryptography

EKE: Encrypted key exchange

A1: Ensure user anonymity

A2: Resist insider attack

A3: Ensure efficient password update

A4: Ensure session key verification

A5: Ensure forward secrecy

A6: Resist denial of service attack

A7: Resist off-line password guessing attack

A8: Resist stolen smart card attack

A9: Resist user impersonation attack

A10: Resist stolen verifier attack

A11: Resist replay attack

B1: User easiness

B2: Scheme complexity

B3: Computation cost

B4: Delay

B5: Communication cost

B6: Mobility in case of smart card/ Biometric scanner

B7: Mobility in case of smart phone

B8: Severity of user compromise

B9: Severity of physician compromise

B10: Provide desired security

B11: Ensure privacy

SI: Security index

UC: User computations

UE: User efficiency

SC: Server computations

SE: Server efficiency

H: High

M: Medium

L: Low

T_h : Time to compute a one-way hash operation

T_{ch} : Time to compute a Chebyshev hash operation

T_s : Time to compute a symmetric/ asymmetric encryption/ decryption operation

T_{pm} : Time to compute a point multiplication/ modular multiplication operation

T_{pa} : Time to compute a point addition operation

T_{minv} : Time to compute a modular inverse operation

T_{me} : Time to compute a modular exponentiation operation

T_f :	Time to compute a pseudo-random function operation
T_H :	Time to compute a bio-hash operation
T_{xor} :	Time to compute an xor operation
$h(.)$:	Hash Function
$H(.)$:	Bio-hash Function
HIPPA:	Health Insurance Portability and Accountability Act
HITECH:	Health Information Technology for Economic and Clinical Health
PHIPA:	Personal Health Information Protection Act
Efficiency :	The total number of operations performed by the user and the server
High efficiency :	Total number of operations ≤ 05
Medium efficiency :	$08 \geq$Total number of operations ≥ 06
Low efficiency :	Total number of operations ≥ 08