INFORMATION SECURITY: A STUDY ON BIOMETRIC SECURITY SOLUTIONS FOR TELECARE MEDICAL INFORMATION SYSTEMS

BY

Ramon Whitman

Bachelors of Science, University of New Hampshire, 2014

Master of Science in Information Technology, University of New Hampshire, 2016

DISSERTATION

Submitted to the University of New Hampshire

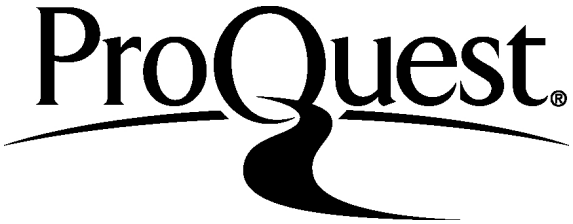
In Partial Fulfillment of the Requirements for the Degree of

Master of Science

In

Information Technology

May, 2016



This thesis/dissertation has been examined and approved in partial fulfillment of the requirements for the degree of Masters of Science in Information Technology by:

Thesis/Dissertation Director, Mihaela Sabin, Ph.D., Associate Professor, Computer Science

Jeremiah Johnson, Ph.D., Assistant Professor, Data Science

Karen Jin, Ph.D., Assistant Professor, Computer Science

Jane Wright, Principal Analyst and Engagement Manager, Security

On April 15, 2016

Original approval signatures are on file with the University of New Hampshire Graduate School.

Contents

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

INFORMATION SECURITY: A STUDY ON BIOMETRIC SECURITY SOLUTIONS FOR TELECARE MEDICAL INFORMATION SYSTEMS

By

Ramon Whitman

University of New Hampshire, May, 2016

This exploratory study provides a means for evaluating and rating Telecare medical information systems in order to provide a more effective security solution. This analysis of existing solutions was conducted via an in-depth study of Telecare security. This is a proposition for current biometric technologies as a new means for secure communication of private information over public channels. Specifically, this research was done in order to provide a means for businesses to evaluate prospective technologies from a 3 dimensional view in order to make am accurate decision on any given biometric security technology. Through identifying key aspects of what makes a security solution the most effective in minimizing risk of a patient's confidential data being exposed we were then able to create a 3 dimensional rubric to see not only from a business view but also the users such as the patients and doctors that use Telecare medical information systems every day. Finally, we also need to understand the implications of biometric solutions from a technological standpoint.

CHAPTER 1: INTRODUCTION

Introduction to Problem

Many patients are in need of medical treatment and need to get in contact with medical specialist whether physicians or doctors. Though this is the case, it is not always easy for those in remote or difficult to reach places. In order to combat such a problem the introduction of telecare medical information systems (TMIS) came to pass. Normally a patient goes to a hospital or clinic, and then consults a doctor, however, "…with the advancement of computer and network technologies, many countries and regions are establishing telecare medical information systems (TMIS), for making the medical diagnosis process more efficient, reliable and effective" (Xie, Dong, & Wong, 2014). With TMIS, patients can have access to doctors and specialists more easily. This in turn provides easier access to patient records between hospitals, clinics, and the patients.

Not all patients can reach their doctors due to distance or health concerns. Though TMIS is needed, it is important to make aware the importance to implement controls in order to make sure sensitive information can be safely transmitted between both parties through public channels. Throughout the years TMIS security has evolved as well as the threats against it. Many studies on current TMIS security solutions; including those within this paper, show that there are faults in their current practices. Current security solutions only seem to be a temporary fix for the problem since hackers seem to find more and more ways to find their way to acquire sensitive information.

Research is already being put in place for the prospective applications biometrics can have for security applications. Biometrics "…based human identification is one of the most

critical and challenging task to meet growing demand for stringent security" (Xie, Hu & Dong, & Wong, 2014). Fingerprint impressions are just one of the many applications for personal identification as well as voice, signature, etc. This study will address the current security risks posed by the use of TMIS by providing a study of current security solutions as well as a study of what types of biometrics exist. This study's goal creates a three dimensional rubric which provides a detailed and accurate analysis of multiple Biometric solutions through the view of businesses, users, and a technical standpoint.

Why Telecare

There is a growing need for better security solutions. Currently there is development being done by researchers in China on TMIS which is explained as:

> With the rapid development of computer network technology, the TMIS provide a way for relating patients, doctors and a medical server. By building TMIS, hospitals try to cut down medical and time expenses and meanwhile make the quality of medical service better. Many patients can be diagnosed at home via TMIS. The medical server owns patients' private medical information such as names, telephone numbers, past medical history and so on. Patients can send instant data of their body to the server via the Internet and doctors can give some advice according to the accumulated patients' health data (Wu & Xu, 2013).

Fortunately there have been many breakthroughs in security with biometrics, which "…provides unique identification methods for the recognition on the basic feature of a human being and it works only when the person to be authenticated [is] to be physically present for the

authentication" (Mishra, 2015). Biometrics is very diverse and therefor has a multitude of applications as it is still being researched.

What is the problem?

Throughout the computer age, security has always been an issue. There are people that are trying to steal sensitive information and put it to use for malicious purposes. We now have a brief understanding of what Telemedicine is and how security relates to it, however, we must understand what a Telecare Medical Information System (TMIS) actually stands for. TMIS, "a Telecare Medical Information System is something that enables or supports health-care delivery services" (Debiao, Jianhua, & Rui, 2011). With TMIS security is important, and with secure security practices and solutions they can be used in order to defend patients' privacy.

Not all current security methods are able to protect against malicious users. There are many security measures that are in place, however, as one new technique or technology is introduced, there is then a new means to beat it. Through careful research the current methods are introduced as an easy to understand list.

1. Smartcard
2. Anonymous three-party password-authenticated key exchange (3PAKE) protocols for TMIS.
3. Elliptic curve cryptography
4. Self-certified Public Keys

These are just some of the many practices that are currently in place and need to be improved upon.

The proposal to address these concerns is through biometrics. Biometrics are a growing form of security that are unique and effective against current flawed techniques. Current technologies for TMIS security face attacks such as replay attacks, on-line password guessing attacks, off-line password guessing attacks, impersonation, and stolen verifier attacks (Wu et al., 2010). These are just some of the many risks that systems face when communicating sensitive information over public channels. This study is done in order to help provide a means for businesses to have an easy, convenient, and accurate tool. A rubric can be used as a means to evaluate the quality of a given security solution. However, we need a deeper understanding on what biometrics as a security solution are as well as their pros and cons. By doing so this study shows finite proof of how this rubric is implemented and how effective it is.

Why we need the study?

The purpose of this paper is to explain these faults and propose the alternate solution of biometrics. Biometrics refers to "the process by which a persons' unique physical and other traits are detected and recorded by an electronic device or system as a means of confirming identity" (Biometrics). There are a multitude of Biometric techniques that enable a new and efficient way to safeguard sensitive medical information. Though there is a wide selection, there are many ways to choose a solution or approach the problem. Whenever a new technology is established it needs to be properly analyzed and rated before a deployment decision can be made. This thesis is created in order to implement a new rating system (rubric) in order to allow businesses and users to make the most effective choice when deciding which security technologies to deploy.

In order to do this however, there is a need to take a further look into what a rubric is, how it is created, and how it can be applied. Rubrics have been used in education as well as

business as a means to evaluate an idea, or in this case, biometrics. Therefore, there is a need for a careful evaluation of existing rubrics and how it can be applied for biometrics, in this instance for security purposes. We do not want a simple one perspective rubric; in this case we create a three-dimensional rubric that will allow evaluating biometrics through the view as business, user, and a technical standpoint.

From a business standpoint a company, in this case a hospital, may desire to implement a TMIS for patients who are hard to reach. However, they want to make sure the information that is being transferred is secure. That is when biometrics comes into to play as a solution for security; however, since biometrics is a newer form of security, it also comes in multiple forms and levels of security it is hard to make a decision. In order to make an educated decision for businesses in the medical field, therefore there is a need to thoroughly research on how effective they will be as given TMIS security solution. This thesis provides a detailed and intricately designed rubric which will allow these businesses to get a thorough understanding of biometric solutions as well an easy and well developed rubric as a reference.

The rubric we need is one which will allow a multidimensional view of biometric solutions. There is not just a need from a business standpoint, but also a need to view how these solutions will affect those working with the TMIS. Users need a secure solution that they can understand how to use. They also need to be able to feel confident that their information is secure. There is also a need to fully understand the pros and cons of each solution as well as the feasibility of each one.

CHAPTER 2 CONVENTIONAL SECURITY SOLUTIONS

A Smart Card Solution

It has already been mentioned that security is a growing concern for any system and therefore there are studies for new security solutions. This chapter was written in order to allow users to better understand what the current security threats are as in order to address security failure. This chapter allows users to better understand what the current state of security is for TMIS, whether they are threats or solutions to these threats.

With the rapid growth of network technology user authentication has become increasingly important. Over the years smart card-based user authentication schemes have been researched due to their low computational cost, convenient portability, and cryptographic properties. The question then is what is a smart card and why are they a widely used means for security?

> A smart card is a device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone…. The reason why the smart card is smart is because smart cards have the unique ability to store relatively large amounts of data, carry out their own on-card functions (e.g. encryption and mutual authentication) and interact intelligently with a smart card reader, with the help of an embedded microcontroller"(Leng, 2009).

Like any other form of security smart cards have had their flaws; however, over the last decade smart card based authentication has been evolving and improving upon these faults. In 2000 two people, Min-Shiang Hwang and Li-Hua Li had first proposed a smart card solution to

an already faulty security measure. The two proposed smart cards that used a scheme based on ElGamal Public Key Cryptosystem that includes the following:

- This is a three phased scheme that begins with the registration phase which allowed new users to establish their identity as well as password calculated and provided with a smart card that contained their password and the functions needed to authenticate.
- The Login phase allows the user to insert the smart card and then input ID.
- Finally, the Authentication phase occurs after the message from the login phase is sent and verified allowing then secure transfer of information (2000).

In 2000, Hwang and Li proposed a solution that "utilized public-key cryptography to propose a remote user authentication scheme with smart cards" (Guo, & Chang, 2013). In 2005 another scheme proposed a robust remote authentication scheme using smart cards. This new scheme did not require either a password table for verification or a clock synchronization between the user and the server. Meanwhile, their scheme can resist a variety of attacks.

These are just some of the many improvements that have been made upon smart cards and the schemes they use. What we focus on now is the introduction of smart card-based password-authenticated protocols that utilize chaotic maps:

> Enlightened by key agreement based on Chebyshev chaotic maps, we propose a novel chaotic maps-based password-authenticated key agreement protocol using smart cards that satisfies almost all the benefits of existing authentication protocols with smart cards, including the following characteristics:
>
> 1. The computational cost of the smart card is low;
> 2. The server does not need to keep the table containing IDs and passwords of users;

3. Our protocol can withstand a series of attacks;
4. The user's identity can be well-protected;
5. The common session key can be established;
6. The user has the ability to choose and change his/her password (Guo, & Chang, 2013).

In this academic journal, researchers propose a password-authenticated key agreement protocol based on chaotic maps. Their proposed protocol contains four phases:

1. The parameter generation phase;
2. The registration phase;
3. The authentication phase;
4. The password change phase.

In the first phase, the server needs to choose some parameters as follows:

1. The server chooses a public key scheme based on Chebyshev chaotic maps
2. The server selects a one-way hash function
3. The server selects a symmetric key cryptosystem with encryption and decryption.

In the second phase the user with an identity would like to register or reregister with the server:

1. This is a process that goes step by step using a password and random number using a specific formula in order to submit the final password registered for a given ID over a secure channel.
2. If the ID that the password is being registered to is valid, it moves through further computation.
3. The server stores the data into a new smart card, and issues the smart card to the user.

4. The user stores a random number into the smart card.

After completing this phase, the user and the server can achieve the goal of mutual authentication and establish an agreed-upon session key used in subsequent communication. This is a long and complex process that can be presented in an algebraic form for visual understanding; however, it is best to take a summarized overview in order to avoid confusion for those that are not from a deep computer background. That said, it can be summarized in the following sentences: The authentication phase is a step by step process that uses information stored in the smart card in tandem with the users password as inputs to be used in conjunction with a timestamp. With these inputs there is a touch and go communication with the server as all of the decryption and authentication is done in order to initiate a secure session between both parties.

The final phase documented in this proposal would be the password change phase. In the proposed scheme, if the user wants to change his/her password, he/she performs the following steps: The user inserts his/her smart card into a card reader, enters the old password, and requests to change the password. Then, the user enters the new password. This is all part of a complex step by step process. In the authentication phase there are a multitude of steps as well as equations that are implemented. Like all other phases the smart card plays a key role to the process and in this phase specifically, the smart card is used via the card reader. The user then enters the old password, and requests to change the password. Then, the user enters the new password which results in messages being sent from the smart card to the server.

There are many proposals for new and improved versions of security for TMIS. For this proposal specifically we can see huge improvements from its predecessors. For instance, usually in a password-based authenticated key agreement protocol, "…during the registration phase, the

user submits his/her identity and password to the server in a secure channel. Then, the server records this message in a password table stored" (Guo, & Chang, 2013).

In this proposal we see that a password table can easily be revealed if the server is compromised. The solution to this was a verification table which still resulted in paying for the maintenance cost and suffering from the password-guessing attack. This proposal of security fixes these flaws through encrypting the verification information using the user's master key and storing into his or her smart card.

Anonymous three-party password-authenticated key exchange

We have talked about chaotic mapped encryption based on smart card usage; however, there are many other forms of security for TMIS. In the next case the security solution is known as anonymous three-party password-authenticated key exchange (3PAKE) protocols. The 3PAKE protocol is "…to achieve mutual authentication between a patient and a doctor with the aid of the trusted medical server (TS), and at the same time, ensure that an adversary does not know the exact identities of both the doctor and the patient" (Xie et al., 2014). Furthermore, 3PAKE is then used for building a secure channel between the patient and the doctor.

In 2007, Lu and Cao had proposed an efficient 3PAKE scheme. However, it was later shown through a study that this scheme was vulnerable to undetectable on-line dictionary attack, off-line password guessing attack, and man-in-the-middle attack. In 2009, Huang proposed another 3PAKE scheme, which was later shown that it could not defend against undetectable password guessing attack and off-line password guessing attack. The list can go from one study to the next, each improving on its predecessor. The study we look at is a 2014 study done by Xie, Hu, Dong, and Wong titled *Anonymous Three-Party Password-Authenticated Key Exchange*

Scheme for Telecare Medical Information Systems. This is a proposal for the first ECC (elliptic curve cryptosystem) based anonymous 3PAKE scheme.

The proposed scheme needs to be summarized due to the many computations done in order to authenticate a user and solidify a session. The whole process can be described as a parallel process:

- Q = A combination of a random number and a generator on Elliptical curve with large order n
- F = This is then used in tandem with the trusted server's public-private key and a random number.
- V = A one way hash of the patients password, ID and doctors ID
- Z= The result of which is used to encrypt the patient and doctors ID as well as a V using the key 'F', are then sent to the trusted server.

Then Q and Z are sent to the server and once the message is received by the server, the server then uses it for the second step.

The second step is when the server takes the message of Q and Z and takes combination of the public-private key and Q. Next, they decrypt Z in order to obtain the IDs of both the doctor and patient as well as V. The server then must verify the users and in order to do this the server takes a one way hash of the patients password, ID and doctors ID in order to compare the V obtained from decrypting Z. If the results do not match those obtained from the message then the session is terminated. Otherwise, the server then knows that there is a desire to establish a shared session key and communicate with the doctor or nurse.

There is a need to verify the doctor in order to establish a shared session key and communicate with the doctor. In order to do this, the trusted server use a random integer TR

exclusive OR operation and hashes the trusted servers ID as well as the doctor's ID and password. This is then sent with the trusted server's ID to the doctor in order to communicate from the doctor's side.

The messages can be summarized as patient to server, server to doctor, and now doctor back to server. Previously we took a random integer TR and now we do the opposite, we calculate TR.

- Next is QB which is equal to when we use a new random number TN and use it in tandem with "a generator on Elliptical curve with large order n".
- FB equals TN and the public-private key.
- We then set VB to equal the hash of doctor password, server and doctor ID, and TR.
- Finally is ZB which is the encryption of the doctor ID and VB.

The doctor then sends QB and ZB back to the server which is then used in the next step of the process.

When the server receives the doctor's message the server must then take QB and calculate FB2 which is the public-private key and QB.

- Afterwards the server decrypts ZB to obtain VB and the doctor ID.
- The server must calculate VB2 which is to equal the hash of doctor password, server and doctor ID, and TR. and then compare with the one obtained from the message
- If the decrypted VB not equal to VB2 then the session is terminated, however, if they are equal then the doctor is authenticated.

The last part of this step can be split into two distinct parts that are for the doctor and the patient. In the instance of the patient we send RA which is the encrypted QB, user and doctor ID, and F. For the doctor we encrypt and send Q, user and doctor ID, and FB.

Upon both parties receiving their respected message they then decrypt. The patient validates that they have the right F and hashes TN and QB as well the user and doctor ID to generate the session key. The doctor then validates that they have the right FB and hashes TN and Q as well the user and doctor ID and calculates the same session key shared with the patient.

This scheme proves to be a new and effective means of security against different modes of attack. The first and most common attempt of attack would be Offline password guessing attack. With this type of attack, a malicious user eavesdrops a communication between the patient, doctor, or trusted server and in turn manages to acquire all the transmitted messages for the session. With these messages a malicious user would try to initiate an offline attack. To launch the off-line password guessing attack, the adversary may choose a trial password and compute, V, the hash of the patient's password as well as the ID of the patient and doctor. However, if the attacker were to even know the doctor and patient ID they would still be unable to compute the encryption of their IDs and V. As the process continues and the attacker tries to verify the data they obtained in the messages they will be unable to verify the password.

The scheme of the study can resist offline attacks as well as perfect forward secrecy. In cryptography perfect forward secrecy is a property of secure communication protocols: a secure communication protocol is said to have forward secrecy if compromise of long-term keys does not compromise past session keys. An example would be where if an adversary "can get TS's secret key *d*, A and B's passwords and identities, the adversary cannot compute the previous

established session key due to the intractability of ***Computational Diffie-Hellman (CDH) problem***.

Another well-known type of attack is a replay attack. Suppose that an adversary impersonates the patient and replays the patient's message to the trusted server, the adversary cannot compute the session key without knowing the random number that has been stored on their smart card. On the other hand, if an adversary impersonates the doctor and replays the doctor's message to the trusted server, the values of the message cannot pass the authentication checking by the trusted server as its random number is a new nonce chosen by trusted server in each new session. The same reason applies if an adversary replays trusted server's messages. The replayed message cannot "…pass the verification performed by the patient and doctor, as their random numbers are new nonces" (Xie et al., 2014) chosen by both individual parties and F and FB are refreshed in each new session.

One of the most common types of security attacks would definitely be Forgery attack and impersonation. However, there is no need for worry in this scheme since it is protected from these kinds of attempts. In the given scheme when an attacker tries to send a message to the patient, doctor, or trusted server impersonating as one of the three they will be unable to authenticate. In this case the messages will be unable to pass because the attacker will not have the password or secret key and as a result will fail in their attempt.

The last type of attack any secure system may face would definitely be a Man-in-the-middle attack. This is a well-known type of security attack, however, the 3PAKE scheme is an effective defense for such a situation. If an adversary attempts to launch the man-in-the-middle attack, the adversary has to "…generate and send the forgery messages to the trusted server and has to pass the verification performed by the trusted server, before the adversary can obtain the

session key shared with the patient and another session key shared with the doctor" (Xie et al., 2014). However, it is an impossible attempt due to the adversary not knowing the secret key or the patient or doctor's password.

ECC-based authenticated key agreement scheme

To protect the transmission of sensitive medical data, a secure and efficient authenticated key agreement scheme should be deployed. The proposal of this next study is an ECC-based authenticated key agreement scheme. We have already mentioned elliptic curve cryptography for TMIS with the previous study; however, this study is different than a 3 way authentication. Security is important and though may be some similarities between security schemes there is also a distinctness that can set them apart.

In this study on ECC-based authenticated key agreement scheme we first take a look at its predecessors. In 2014 there was a proposal by Xu, X., Zhu, P.,Wen, Q. Y., Jin, Z. P., Zhang, H., and He, L. in their, (*A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information system*) for an ECC based authenticated key agreement scheme for TMIS. This proposal was claimed to be secure and efficient. However, a follow-up study by Islam and Khan pointed out that Xu et al.'s scheme has:

1. It fails to check the wrong input in login phase, which will cause unnecessary communication and computational costs;
2. It lacks of correctness verification on old password in password change phase where this weakness will lead to a denial-of service attack.
3. It cannot resist the strong replay attack
4. It does not provide the revocation for the lost or stolen smartcard

Though they sought improvement, Islam and Khan failed to see the faults in their own work. This study documents faults in the two's schemes as well as a new and improved ECC based authenticated key agreement scheme. Islam and Khan's scheme is a six phase scheme: initialization, registration, login, authentication, password change, and lost/stolen smartcard revocation phase. Though this scheme improves on the previous faults it fails cover its own problems of providing user anonymity, protect against spoof attacks, off-line password guessing attack with a smartcard, impersonation attacks, man-in-the-middle attacks, modification attacks, replay attack and strong replay attacks.

There is a need for maintaining a secured TMIS system. This solution provides a new and improved scheme to supplement for the current faults in the existing solution. According to Islam and Khan's proposal their protocol fails to resist several attacks since the secret value public key is shared by all legal users. To erase these security flaws, they proposed an ECC-based authenticated key agreement protocol. The proposed protocol consists of six phases: initialization, registration, login, authentication, password change, and revocation of lost or stolen smartcard.

The initialization phase the server "chooses an elliptic curve Ep(a,b) over a prime finite field Fp and a base point P over Ep(a,b)". (Zhang, & Zhu, 2015) The server then selects a high entropy random integer as its private key and uses it to compute its public key. Then, it chooses a secure one way hash function. The server keep secret key secret and publishes the needed information

The registration phase is initiated whenever the patient initially registers or re-registers to the Telecare server. "After executing following steps, each user can obtain a smartcard from the server" (Zhang, L., & Zhu, S. 2015). The user chooses its identity and password and generates a

random number for computing *l*, the hash of string concatenation of the password and random number. The user then submits their ID and *l* to the server via a secure channel. In order to register the server must make sure whether or not the provided ID is in the database. If a patient is already registered they will be re-registered otherwise they will be registered for the first time. Once this part of the process is handled a patient is then issued a smart card that holds all relevant information of the random number, Elliptical curve, *l*, a base point of the curve, the secret key, *v* which is the secret key and exclusive OR operation of *l*, and other key values.

When a user accesses the server, she/he inserts the smartcard into the smartcard reader and inputs her/his ID and password. The smartcard computes whether these values match those on the server and if that is the case they maintain the session otherwise it is aborted. In the case key values match the server then selects a nonce, which is an arbitrary number that may only be used once, and a timestamp. There are multiple calculations as well in the login phase:

- *V*, the smartcards the nonce and a base point of the curve.
- A nonce and the secret key the base point of the curve.
- A hash of the concatenation of the timestamp and *l*, the hash of string concatenation of the password.
- *M*¸ the he secret key and exclusive OR operation of *l*, and exclusive OR operation of *l*
- *D* which is the hash of *V* concatenated to *M and* concatenation a previous stored value of the registration phase N
- Finally *G1* which is the encryption of concatenation of *D* and the ID.

With these calculations the smartcard sends a login message with (*V, G1,* and the timestamp) which is used in the authentication phase in order to verify each other.

The authentication phase uses the message generated from the login in phase in order to verify that is a valid transmission the use of the timestamp. With the timestamp the server verifies if the timestamp is valid or has expired. If the timestamp is valid the server takes the other values from the login message in order to decrypt the values and obtain the ID. Once the server has the patients ID it them validates the ID through the comparison of the stored value in its database. If invalid the session is terminated and the patient is informed, however, if the ID is found to be valid further calculations are done in order to validate the patient as a legal user. Finally, the server sends a message back to the patient through a public channel.

In the authentication phase it is also important to note the need to protect against the replay attacks and facilitate the lost smartcard revocation. The server as noted contains the patient's ID registration time, and N which is zero for first registration and N + 1 with every reregistration. If receiving the next login message within a valid time interval, the server checks whether or not Time = Time. If the equation holds, the server rejects the login request as the received message is nothing but a replay message; otherwise, the server updates the tuple (ID, N value, and time. When receiving the authentication message from the server the smart card checks validation of the time interval and calculates for it. If the interval is greater than the transmission delay it smartcard stops the session; otherwise, it computes and compares values of the message with those stored on the smart card and if they are not equal the session is aborted otherwise the patient authenticates with the server successfully.

There are in fact two more phase in addition to the 4 needed in order to establish a successful session. One such phase would be the password change phase. This phase can be separated in to two important parts with the first being smart card computing the hash of the concatenation of the patient's pass word with the random number stored on it. Then, that value is

with the “Exclusive OR operation” and patient’s ID and compares it to the value on the smart card. In such an instance when the value matches then the patient is allowed to change their password. In the second part of the password change phase a new random number and new password need to be stored on the smart card. Using these two values the smart card then must recalculates all important values that were previously stored on the smartcard.

What thing to take note of is what happens in the instance of a lost or stolen smartcard. This instance is defined in the final phase lost/stolen smartcard revocation phase. First, when such an instance occurs the patient must first request the server for its revocation. After that there are two parts to be noted to this phase. First, the patient must choose a new password and random number which are then use to calculate *l* which is a hash of the concatenation of the password and random number. With this value it is then submitted with the patient’s ID over a secure channel to the server. The last and key step is the same as the second phase. In this phase the server checks the registration credentials of the patient. If the credential provided by the patient is valid, the server updates N as N= N+1 for the tuple (patient ID, N, and time of registration) to revoke the smartcard.

Self-certified Public Keys

When it comes to security there are many different approaches to a secure security solution. As a result, businesses must then be made aware that there are constantly studies being made in order to improve upon existing schemes and their faults. So far we presented 3PAKE, chaotic mapped, and ECC-based authenticated key agreement scheme. We elaborate now on a novel authentication scheme using self-certified public keys for Telecare Medical Information Systems.

In this study on Self-certified Public Keys we first take a look at its predecessors. In 2012 there was a proposal by Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C. in their proposal (A secure authentication scheme for telecare medicine information systems) an efficient remote user authentication scheme for TMIS. This proposal was claimed to be secure and efficient. However, a follow-up study by He, D.B., Chen, J.H., Zhang, R., and others prove the point out the flaws of their predecessors. In this paper, they propose an authentication scheme for telecare medical information systems using self-certified public keys. Also in this study, they present a "bilinear pairings-based authentication scheme with privacy preservation for TMIS (Zhang & Zhu, 2015)

It is important to note that the proposed scheme as a whole has proposed the four phases: Registration phase, login phase, authentication phase, and password change phase. However, before we even begin this scheme it is important to initialize the scheme. First the server selects an *G:* additive cyclic group of prime order *q* generated by *P* and then the server selects, *G2* a multiplicative cyclic group of same order *q*. Following that, the server then selects the master secret key and computes for the public key. Finally, the server publishes the system parameters.

The first and most common phase of any scheme would be the registration phase. During the registration phase the first step is for the patient to choose his/her identity *ID*, password and generates *R:* a random number. Then he/she computes *RPW* which is a collision-resistant one-way hash function of the concatenation of that random number and the selected password. Once done, a message containing the patient pass word and *RPW* is sent to the medical server via a secure communication channel. Upon receiving this message the next step is for the server to select *R* which is a random number. With this random number the sever:

1. *AID* secret key and hash of the patient ID
2. *K* hash of AID

3. *J* AID exception or hash of concatenation of *ID* and *RPW*
4. and *CID* encryption of patient ID and *R* where encryption key is the server's private key

The last two steps of the registration phase can be easily summarized. The third step of the four step registration phase would be the authentication phase. During this phase the server personalizes the smart card for the patient with *(J, K, CID, e* a bilinear map, *G, G2, P, q* prime order of *G* and *G2,* the public key of the server) and other values. The last step of the registration phase would be the last value needed for the smart card is added. This value *R2* is the random exception or of a collision-resistant hash of the concatenation of the patients ID and password.

The second key phase of this scheme would be the login phase. The login phase can be broken down into three key steps. The first of this three step phase occurs when the user inserts the provided smart card in order to input their ID and password. When the smart card is put in the reader it then computes

1. *r* which is *R2* exception or a collision-resistant hash of the concatenation of the patients ID and password.
2. *RPW* which is a hash of *r* concatenated to the patients password.
3. *AID* which is (*J* from the smartcard) exception or a hash of *r* concatenated to the patient's ID and *RPW*
4. *K* equals the hash of *AID*

These are done in order to verify *K* equals the one on the smart card of the user in order create or terminate the intended session. The last two steps of the login phase are just as important. In this phase, the smart card choosing *A*, a random number is selected and through this number and

value *P*. Finally the message of the login request is sent to the medical server for authentication containing *A, B,* and *CID*.

In the third phase of authentication, upon receiving the message from the patient the medical server takes those values and decrypts the value *CID* using the master secret key in order to obtain the patient's ID. If it is invalid, the server aborts the login request; otherwise, it compares *B* with the computed *e* that is calculated through a bilinear map of a secure one-way hash function of the patient's ID and the master secret key and *A*. If the computation holds, the patient's legitimacy is assured, otherwise the session is aborted. Subsequently, the server generates two random numbers *b* and *R'* to compute *CID* which is equal to the encryption using the master secret key of the two values *R'* and the patient's ID. Then, they create *Cs* which is equal to b and P, *sk* which is equal to a hash of *b A* concatenated to *AID*. Finally, we obtain *Vs* which is equal to a hash of a secure one way hash function of the patient's ID concatenated to *sk*, *AID*, and *CID*. With this, the server sends a mutual authentication message to the patient.

Upon receiving the reply message the patient computes for *Vs* in order to compare said calculation with the one in the message. If matched, the medical server is authentic otherwise the login request is given up by the patient. However, if it is authentic the patient then computes for the session key using the values found in the reply message and sends it back to the server and stores *CID* by updating the smart card value. Once the medical server has received the patient's message it then verifies whether or not the session key equals to the value gets from a hash of a concatenation of *sk* and *CID*. If the value holds, the mutual authentication is completed otherwise the whole process fails. Finally the patient and medial server both share the common session key for the further communications.

The final phase is the password phase which is key noted a three step process that is implemented when a patient needs to change their password. When a patient wishes to change their password they must first enter their smartcard into the reader and then request a password change. The smartcard computes the same values it computed for the log in phase first step and checks whether *K* equals the hash of *AID*. If the equation holds the user proceed to the next step otherwise the password change phase is terminated. The last step of this phase is the easiest to understand since all that needs to be done is for the new password to be added twice for correctness and then the smartcard recalculates the values it will store.

Like our previously discussed schemes this scheme also shows improvement upon its predecessors through lack of vulnerability against different attacks. In order to maintain a user's privacy, the solution must be able to fair against off-line password guessing attack, replay attack, forward secrecy, and other known security threats. The first thing we mentioned was patient's privacy protection which is important because the information that is being transported over public channels is sensitive medical and personal information. In this study we can quote that the attacker has "no ability to trace the moving history and current location of the patient according to the varied login request message, which combines with random numbers in each session'. (Zhang & Zhu, 2015)

CHAPTER 3 CURRENT BIOMETRIC SOLUTIONS

Finger Prints

One of the most widely known and common forms of biometrics are fingerprints. However, we first must understand what biometrics are. Biometrics are human characteristics. By using these human characteristics biometrics authentication is used as a form of identification and access control. Biometrics are very diverse with its many forms and intricate applications.

Fingerprints are something that everyone has and are something that are unique only to the person they come from:

> The fingerprints impressions have been used for personal identification for over 2000 years and automated fingerprint identification systems have been used for decades. Compared with other extrinsic biometric features, fingerprint is considered to be the most invariant and reliable and occupies the largest share in the global biometrics market. Nearly all forensics and law enforcement agencies worldwide utilize Automatic Fingerprint Identification Systems (AFIS) (Kumar & Kwong, 2015).

That said, this makes fingerprints an optimal source of security. Throughout the years, there have been three key noted means for fingerprint biometrics. These include touched based 2D Fingerprint, contactless 2D fingerprint, and contactless 3D fingerprint.

In order to gain the benefits of higher use, "convenience, hygiene, and improved accuracy, contactless 3D fingerprint recognition techniques have recently been introduced in many literatures" (Kumar & Kwong, 2015). The traditional acquisition of fingerprint scans were done by pressing or rolling of the finger against "…[a] hard surface (glass, silicon, polymer) or paper [which] often results in partial or degraded quality images due to improper finger

placement, skin deformation, slippages, smearing or sensor noise" (Kumar & Kwong, 2015). Originally these fingerprints were done as live fingerprint scans for commercial and law-enforcement applications; however, with growth in technology, the uses are becoming more widespread and diverse.

The problem with the traditional method of 2D fingerprints was often due to having to cope with the residue of dirt, moisture, and sweat left from the previous fingerprint scans. As a result, there was a need for manual cleaning of the sensor surface. On the other hand, there was the introduction of the contactless or touchless 2D fingerprint systems. These systems allowed for the avoidance of direct contact between the imaging sensor and the elastic finger surface. This new form of scanning allowed for the fingerprint imaging to avoid fingerprint deformation and achieve higher accuracy in the automated fingerprint recognition.

Unlike the simple 2D touch based fingerprint, Parziale and Chen have proposed "a contactless fingerprint identification system that uses multiple cameras to systematically acquire multiple views of the presented finger" (Kumar, 2015). By taking multiple views they are then combined to reconstruct a 3D representation of the desired fingerprint. The core technology in this system is based on the "shape from silhouette, which requires views of fingerprint from different viewpoints and under different illuminations" (Kumar & Kwong, 2015). These silhouettes are used in order to construct an accurate the 3D representation of the desired fingerprint.

Accuracy is important and using proper technology and techniques are needed in order to provide an accurate and therefore secure form of security. In order to have an accurate 3D representation of a fingerprint, there was therefore a need for multiple cameras to replace the conventional 2D fingerprint system. This kind of system, though accurate, results in a high cost

system. What is normally desired for any system would be a simple, yet accurate system that would not burn a hole in a company's budget.

These high priced systems will therefore be ineffective to companies that need a secure and accurate system. A traditional 3D fingerprint system could have up to five cameras and require things such as a specialized projector and a high-speed camera to implement 3D fingerprints. This therefore provides a strong motivation and need "…to develop low-cost solutions for 3D fingerprint identification" (Kumar & Kwong, 2015). One such solution would be a 3D fingerprint system that uses a single fixed camera.

In 2015 there was a proposal for such a system, showing that there were already improvements being made on the 3D fingerprint design. Such a system uses a calibrated setup of multiple light (LED) sources in space that light in a specific sequence to acquire the needed 2D fingerprint images. Once these images are gathered there then comes the most important part, which is reconstructing them into a usable 3D image. This is not a simple process; it requires specific lighting, angles, and mathematic formulas in order to develop the desired result.

When it comes to fingerprints there are more than one given application. Fingerprint security is evolving, and its uses for security are becoming more diverse. A 2013 study shows the convenience and commonality of smartphones and how biometrics can apply to this technology. A smart mobile phone is capable of connecting to other devices, with the help of different applications:

> Consequently, with these connections comes the requirement of security to protect personal information. Nowadays, in many applications, a biometric fingerprint recognition system has been embedded as a primary security measure. To enable a biometric fingerprint recognition system in smart mobile phones, without any additional

costs, a built-in high performance camera can be utilized. The camera can capture the fingerprint image and generate biometric traits that qualify the biometric fingerprint authentication approach. However, the images acquired by a mobile phone are entirely different from the images obtained by dedicated fingerprint sensors (Khalil, Kurniawan, & Saleem, 2013).

Though a promising solution to security, fingerprints are becoming a challenge. One reason is due to the degree of freedom in the mobile camera which is greater than the 2D touch-based sensor. There are other concerns with this technology due to a variance on image focus, rolling, pitching and distance. With the fingerprint itself "…the ridge and valley information of the fingerprint image is also greatly dependent on the aspects of the camera used. The contrast of a ridge and valley is fragile, when compared to the touch-based sensor." (Khalil, Kurniawan, & Saleem, 2013). As a result of that, the capturing of the fingerprint image using a mobile phone is "…totally erratic, as the entire process depends on how, where and when the user clicks to authenticate" (Khalil, Kurniawan, & Saleem, 2013).

As stated, acquiring the fingerprint image using a camera will produce high variability and inconsistency images due to camera pixels and the position of a finger. The process of smart phone based security is not just a simple scan and submit to the system. In fact, it is a detailed, multistep process that is done in order to provide as much accuracy as possible. "The ridge structure of a finger is crucial information for recognition purposes. Extracting the ridge and valley is required prior to feature extraction" (Khalil, Kurniawan, & Saleem, 2013). There are many other steps to this process, however they are all key in order to provide as accurate print as possible.

Though we can acquire and process a fingerprint, in reality no fingerprint recognition system can give 100 percent accuracy about the individual's identity. Instead, a fingerprint provides the individual's identity with "…a matching score ranging in the interval of {0, 1}" (Khalil, Kurniawan, & Saleem, 2013). When this matching score is closer to 1 in the system, then it can be inferred that more than likely the fingerprints come from the same finger. However, on the other end if the score is closer to 0 then it is highly likely that the fingerprints do not belong to the same finger. On a more technical standpoint, studies show that a system is synchronized by a threshold *t*. Fingerprints are only considered the same when the matching score is higher than or equal to the threshold *t*.

Ocular biometrics

With the increasing need for better security, there is therefore a diverse selection of biometric security solutions to evaluate. Traditional approaches such as the use of identification cards, passwords, or PINs are becoming inadequate and therefore there is a need for a secure and evolving method. It is stated that fingerprint biometrics is a plausible solution due to its security and diverse applications.

> Biometrics refers to the "use of physiological and behavioral characteristics of humans for establishing their identity. Among physiological characteristics, several body parts have been studied that demonstrate biometric properties such as universality, uniqueness, permanence, and collectability. ....The ocular region, including iris, is one of the most stable ones and can be effectively used for recognition." (Nigam, Vatsa, & Singh, 2015).

That said, there is need to take a closer look at these forms of biometrics.

The field of ocular biometrics has made significant progress in the last decade. Many researchers have developed a number of diverse techniques to utilize the information found in

the human eye. The eye is an important organ that is made of multiple components such as the cornea, lens, optic nerve, retina, pupil, iris, and the periocular region. Out of these, the "…iris, periocular, retina, and sclera have been well studied for being potential biometric modalities" (Nigam, Vatsa, & Singh, 2015). There has been continuous study over the years, with iris recognition study started back in 1987. From there we see study followed by sclera, retina, and then periocular recognition starting in 2009. Through these studies there have been many key contributions done in order to improve the ocular related biometrics we see today.

When one thinks of ocular biometrics they would then think of those related to the iris. The iris is known as the precursor of biometrics and the fact that the iris may be used as an "…optical fingerprint" (Nigam, Vatsa, & Singh, 2015) was first explored by Flom and Safir in their study *Iris Recognition System*." Since 1987, iris recognition has evolved into a reliable biometric trait and has been extensively studied by the biometric research community. It has even come to the point that there is large-scale deployment of "…commercial and public iris recognition systems around the world. One of the foremost examples of such a system includes the Aadhaar Unique Identification Authority of India (UIDAI) Program, which performs approximately 100 trillion iris matches every day" (Nigam, Vatsa, & Singh, 2015). The process of an iris recognition system involves acquisition, preprocessing, segmentation, feature extraction, and matching.

Acquisition is one of the most important parts of an iris recognition system since without an accurate and decent quality scan the system will have nothing to work with. Many studies over the years, by people such as McCloskey et al., (2010) who explored the problem of capturing sharp iris images from subjects in motion. Tankasala et al. (2012) were another group of people who "…design and implement a hyper-focal imaging system for acquiring iris images

in the visible spectrum." (Nigam, Vatsa, & Singh, 2015) These studies are all big contributions to modern day iris recognition. With regards to the current acquisition systems are generally constrained towards:

1. Capturing images at a distance of approximately one feet.
2. Increasing the usability of the iris as a biometric, researchers are attempting to design hardware that can capture good quality images without requiring significant cooperation from the user (Nigam, Vatsa, & Singh, 2015).
3. Designing a system that can function as a ''…walk through'' recognition system" (Nigam, Vatsa, & Singh, 2015).

In recent years, iris recognition has moved towards real-word applications. Due to the difficulties of image acquisition, current research have shown the importance of "…quality assessment and preprocessing of biometric samples" (Nigam, Vatsa, & Singh, 2015). Researchers now face this challenge of imperfect images and as a result there is now a need for "…quality assessment based pre-processing techniques to be applied to them prior to recognition" (Nigam, Vatsa, & Singh, 2015). Though important, segmentation approaches are the next key point in the iris recognition process:

> Iris sensors acquire not only the iris but also some surrounding regions. Depending on the acquisition device, the amount of neighboring regions varies. Therefore, it is important to have a robust iris segmentation algorithm… Researchers are also actively pursuing the development of novel non-linear algorithms to meet the demands of the increasing complexity of iris biometric systems (Nigam, Vatsa, & Singh, 2015).

Matching and indexing are the final point to iris recognition. "Advancements in the field of iris recognition have led to the adoption of a number of feature representations for iris

information" (Nigam, Vatsa, & Singh, 2015). Over the years matching techniques have also evolved along with this "…diversification in iris representation" (Nigam, Vatsa, & Singh, 2015). Large-scale deployment of iris recognition systems around the world has inspired researchers to develop efficient and cost effective template matching techniques.

There are many factors that can impede a clean and accurate iris scan. The unconstrained environments involving noise, non-cooperative subjects, occlusion, and other non-ideal scenarios give birth for research on other forms of ocular biometrics:

> In 2009, Park et al. proposed periocular as a novel biometric trait. The periocular region is defined as the part of the face surrounding the eyes. This principal investigation, performed in the visible spectrum, studied the efficacy of the trait using global as well as local descriptors. The results of the study have motivated the research community to actively explore the periocular biometrics in diverse scenarios (Nigam, Vatsa, & Singh, 2015).

This opens ups a whole new and promising form of biometrics.

Periocular features can also be used for more than just security but also a means to determine gender, age, and ethnicity of subjects. Current research is at a point where periocular recognition can be used in instances when iris recognition fails. We can see from studies that this form of recognition works on verifying and identifying users through their periocular region (area around the eye).

There are three key parts to take note of when we talk of periocular biometrics. Verification and identification, soft biometrics, and human performance evaluation. Of these three, verification and identification using the periocular region is important in order to

effectively identify and authenticate users. For verification and identification, there are many studies that propose techniques and technologies to be used in periocular authentication.

One such study was done by Proenca et al. which shows an approach to periocular recognition through defining the periocular region into multiple components consisting of the iris, sclera, eyelashes, eyebrows, hair, skin and glasses. "A group of classification models predicts the posterior probabilities for each pixel in the periocular region for it to belong to one of the above component classes. The appearance based information is fused to geometrical constraints and shape priors to feed a two-layered Markov Random Field" (Nigam, Vatsa, & Singh, 2015). Another study by Juefei-Xu et al. (**who**) shows a feature extraction approach on periocular regions to "…address the age-invariant face recognition problem. Images from the FG-NET dataset are pre-processed for illumination and pose correction, and periocular region normalization" (Nigam, Vatsa, & Singh, 2015).

Periocular authentication is studied as one of the many types of ocular recognition. Current research of periocular biometrics shows:

1. Cross-spectral periocular recognition: Periocular recognition is used in conjunction with face recognition in the presence of occlusion. The periocular region is also critical in ocular recognition when the iris fails in unconstrained scenarios. Since iris recognition and face recognition are traditionally performed in the NIR and visible spectra, respectively, one of the important directions of re-search is to perform periocular recognition across spectra to potentially allow these modalities to work together (Nigam, Vatsa, & Singh, 2015).
2. Anti-spoofing measures: One of the factors on which acceptability of a biometric trait depends for real-world applications is its resilience to spoofing attacks. It is required that

the biometric community focuses on establishing measures to minimize spoofing of the trait (Nigam, Vatsa, & Singh, 2015).

3. Unconstrained recognition at-a-distance: Among all ocular biometric modalities, the periocular trait requires the least constrained acquisition process. It has the potential to allow ocular recognition at large stand-off distances, with applications in surveillance. It is likely that the research community will move towards exploring ocular recognition at a distance in more detail as compared to present studies (Nigam, Vatsa, & Singh, 2015).

Another known type of ocular recognition is retina biometrics. Known as one of the most secure forms of ocular biometrics, this form of biometrics "is believed to be the most secure biometric modality as it is extremely difficult to spoof the retinal vasculature" (Nigam, Vatsa, & Singh, 2015). Studies by Arakala et al. found that a retina vessel could be used to compare patterns using error-correcting graph matching. Arakala et al. also observed that

> …apart from nodes, three other graph sub-structures are suitable for separating genuine comparisons from impostor comparisons….. Experiments on the VARIA database show that using nodes as feature points, edges, and paths of length two units result in match scores which completely separate genuine from impostor comparisons (Nigam, Vatsa, & Singh, 2015).

This in turn shows that retina biometrics is harder to attack then other ocular biometrics.

Behavioral biometrics: The signature

There are many different biometric traits that have been proposed and studied for user verification. One category of biometrics is known as behavioral biometrics which uses behavioral attributes such as signature, gestures, voice and keyboard as a means to authenticate users. The one that we specifically look at would be the human signature.

> Among the different biometric traits that have been proposed and studied in the literature, automatic handwritten signature verification stands out as one of the most attractive due to its social and legal acceptance, derived from the wide spread use that has traditionally been given as a personal authentication method (Gabally et al., 2015).

This form of biometrics has been studied for a long time; however, "…the practical deployment of this technology has been slower than what was foreseen some years ago, as its performance remains a step behind other largely used traits like fingerprint or iris" (Gabally et al., 2015). Why? Well, there are three points to behavioral biometrics such as a signature that led to this:

1. Difference among samples of the same individual is usually higher than physiological biometrics traits such as the iris or a fingerprint.
2. "Learned traits such as the signature present a relatively low permanence overtime, which decreases the accuracy of recognition systems …The fact that a signature is something that we can learn to produce opens two different impostor scenarios" (Gabally et al., 2015). Some examples include:
    a. Random impostors, these are common to all biometrics, they are attackers that try to access the system with a false trait, in this case signature, in an attempt to pose as another user (Gabally et al., 2015).

b. Skilled impostors: In the case of behavioral biometrics this is the instance an attacker learns how to reproduce the user's trait (ie. signature). In this instance the attacker has enough information to imitate the user and therefore try to access the system (Gabally et al., 2015).
c. "Such skilled forgeries usually lie inside the subject's intraclass variability leading to a significant decrease of the recognition performance. This operational framework is especially relevant in forensic related applications (e.g., signature forgery detection in checks or official documents)" (Gabally et al., 2015).

As result to these three points it is apparent that a signature as a form of biometric is very challenging to research.

Signature biometrics can be split into two distinct modes, on-line or dynamic signature and off-line or static signature. On-line signature is traditionally based

> …on the time functions produced during the signing process (e.g., position trajectories or pressure versus time), acquired using devices like touch screens or digitizing tablets while off-line or static signature recognition, based on the static image of the signature, usually digitalized from a hard copy document (Gabally et al., 2015).

As a result, many dynamic features can be captured; however, the question is which features should be preferred in verification? Since signatures are a behavioral based biometric, there is therefore a need to choose the features that "…have the greatest discriminant factors. The modern tablet is capable of measuring many dynamic features such as pressure of a pen on the tablet surface, position of a pen, velocity, acceleration, and so on" (Doroz, Piotr, & Tomasz, 2015). Dynamic signature features are important, and with these signature features we are able to

distinguish a given signature from all other signatures when compared to those in a database or other data source.

Between the two, on-line signatures are usually known as the more accurate version due more information being available. Both methods have their own approach, however, research from other studies show the best method of authentication would be a combination of the two. Though the optimal choice, the combination of both on-line and off-line recognition has not been implemented as much up untill now due to the amount of effort needed to accomplish it. Now though, a recent study, *On-line signature recognition through the combination of real dynamic data and synthetically generated static data*, proposes a solution to this dilemma.

> In particular, we describe a new method for the synthetic generation of static samples from their real dynamic instances. This method allows us to incorporate certain on-line information from the real signature (e.g., the speed, the pressure or the pen- ups trajectory), to the synthetic static image in order to increase its discriminative power especially in the presence of skilled forgeries. Then, synthetically generated off-line data are used within a novel on-line recognition architecture to enhance the performance of current top-ranked dynamic signature verifiers, comparing the accuracy of the new proposed approach with traditional fusion techniques based only on real data (Gabally et al., 2015).

Signature biometrics is evolving from the current standard of off-line and on-line biometrics. Studies such as *On-line signature recognition through the combination of real dynamic data and synthetically generated static data* show that these two forms of signature biometrics have been proven to be incomparably weaker to the fusion of the two. The fusion of

both forms of biometrics has shown a decrease in error rates. This method attempts to solve the problem of both on-line and off-line structures, by taking the best from both.

Behavioral biometrics: The Human Voice

Voice biometrics are a technology that identifies a user based on their unique voice characteristics. There are many components that makes a voice unique, i.e. the structure of the vocal chords, the trachea, the nose, the placement of teeth. All these characteristics are what makes a person who they are as well as a password that "…cannot be falsified or transferred. Biometric technologies do not rely on what you know, or what you possess, but rely on what you are" (Khitrov).

There are two types of voice recognition: text dependent and text independent. With a text dependent speech, a user has to speak exactly the enrolled or given password. On the other hand:

> Text independent verification accepts any spoken input, making it possible to design unobtrusive, even invisible, verification applications that examine the ongoing speech of an individual. The ability of text independent technology to operate unobtrusively and in the background makes it attractive for customer related applications, because customers need not pause for a security check before moving on to their primary business objective (Markowitz, 2000).

All biometrics are unique, but what sets voice biometrics apart from the rest would be "…its contactless application. Unlike fingerprints, voiceprints can be taken remotely" (Khitrov). This means that voice biometrics has the possibility for a wide array of applications i.e. while driving, from another room or even through the use of mobile devices. Voice biometrics use is

very simple; the user says a passphrase that is used in order to be matched against those stored in a database:

> The matching procedure generates a score representing how accurately the new utterance matches the stored voiceprint. Access score thresholds can be pre-set for enhanced security. For instance, if a match procedure generates a low score, match access will be blocked. One more reason to trust voice biometrics as a passkey technology is its simplicity; after all, we speak all the time. With voice biometrics, a person only needs to do what comes naturally to confirm his or her identity, for instance, say his or her name, telephone number or repeat a prompted phrase (Khitrov).

Though voice biometrics may sound like the optimal choice, like all other forms of biometrics it faces some sort of challenges:

1. Environmental noise, which varies as to noise type and level (Khitrov).
2. Presentation effects, including speech sample duration, the psychophysiological state of the speech (ie illness and emotions), and effects of vocal strain (Khitrov).
3. Channel effects including interferences and distortion (Khitrov).

What sets voice recognition a part lies with the fact that a voice cannot be stolen, and voice recordings can't be used to falsify authentication. A fusion of biometric techniques is even beginning to be used as a means to make up for faults in different forms of biometrics. By combining key components from different modalities we are then able to achieve as close to 100% security as possible. "For example, if a device first asks for your fingerprint and then asks you to repeat a combination of numbers aloud, there is zero chance that an unauthorized person will be able to access your device" (Khitrov).

Such a simple technology allows an ease of implementation. Today there many forms of modern mobile devices such as a phone or tablet that have built-in microphones. Smart devises are common place and used for anything from banking to sharing photos. As a result of the growing use of smart devices there is the need to secure sensitive information from unwanted parties. As a result, there is a growing need for security. Voice biometrics provide unique security and as a "….added convenience is that voice biometrics can be run on a remote server, 'in the cloud' and not on the user's own device. In this case, even if a device is lost, stolen or misplaced, the unique voice characteristics associated with it are not lost, stolen or otherwise compromised. (Khitrov). Like all forms of security, there are faults, however, as a result there is also constant growth and development.

Chapter 4 MULTI-DIMENSIONAL BIOMETRIC EVALUATION

Business

Security it is important, something that ensures our information is safe. Currently security is lacking for Telecare medical information systems and therefore there is now a need for a better alternative solution. Chapter three proposes biometrics as the new better alternative to current TMIS security solutions. That said, how do we know which biometric solution is best, does it keep our info safe? This thesis builds upon these ideas in order to generate a three dimensional rubric that can be used from a business, user, and technical standpoint in order to make the most educated decisions for TMIS security solutions.

A hospital is a business, and like any business we want to implement security controls that are technically effective and cost effective. Businesses should consider four attributes when a decision needs to be made about a Biometric solution. These categories include security, rate of growth and development, applications, and costs and ease of implementation. These four categories are then broken down into four degrees of 4 = excellent, 3 = adequate, 2 = fair, and 1 = minimal.

Table 1. Business Rubric

	4 = excellent	**3 = adequate**	**2 = fair**	**1 = minimal**
Security				
Development				
Applications..				
…Implementation…				

Rating Security

There is a need for security when transporting sensitive information over a public channel. However, there is a need to understand what security is from a business perspective. To

a business, security is when a system is protected from attackers, hackers, or malicious users. The protection can be the hardware used or the software programed to prevent illegal access.

Within the scope of the biometrics we discussed we can see a varying level of security efficacy, whether it is physical or behavioral biometrics. A rating of four on a scale of 1 to 4 represents an excellent security solution since it represents a level of security where there is only a small to null susceptibility to attacks and chance for a compromised TMIS session. Another key component when it comes to a security solution is that it has as a proven history of effectiveness.

When it comes to security there are many features, parameters, and components that make it secure. There therefore a need to understand whether the system is truly secure. In telecare medical information systems, as in our example, a rating of 4 means that when hackers, attackers, or any person with malicious intent attempts to illegally access our system will be unable to do so. This means that a form of biometrics is secure due to its unique characteristic that makes it hard to attack and it has multiple precautions set in place in order to avoid failure. This also means that the form of security has a long history of little to no security compromises due to attacks.

A rating of 3 on our rating scale represents an adequate security solution. This means that attackers may be successful a small percentage of the time. This also means that a given biometric security solution has had a history of some failures which it has improved upon and has solved.

A rating of 2 represents only a fair level security solution. This means that it is susceptible to attacks, making it not very secure for a given session, with a marked history of failure. An example of this is when we look at the long history of signature biometrics. Signature

biometrics have been deployed in many forms to implement security, however, skilled imposters have compromised these signature-based solutions. Though this has happened, these solutions are still rated fair because there are studies that indicated developers have improved upon these faults and proposed new and better methods to implement security.

A rating 1, is known as a minimal level of security. This the lowest rating a security solution can possibly can achieve. This also means that with any given form of biometrics it has a long history of failure and is frequently susceptible to attacks. When proposes new and improved security solutions are proposed for the given form of biometrics a new method of attack has been found to thwart it.

Development

Technology is always evolving, and with it, a growing danger for private information to be stolen. We have already touched upon the importance that security has for a biometric solution, however, we have yet to mention the importance of development of a security solution. Both security and development must be implemented side by side. When a security solution is attacked and breached due a security flaw or a new invented means of attacking is found, a system is at risk. This is why rate of growth in development is important because it shows whether or not there is constant work being done to improve, evolving upon an existing system.

An excellent biometric solution is one that is always being improved upon. This means that there is a constant effort to improve upon the current solution, an effort to improve upon security, ease of use, accuracy, and other quality attributes. An example of such a solution would be signature biometrics. We have seen that originally signature biometrics consisted of on-line and off-line forms. Both forms of this type of biometrics had their pros and cons, however, this

form of biometrics has shown that over time there has been a constant effort to improve the technologies itself for better security through a fusion of both.

The highest rating any category can receive is a 4, also known as excellent. When we talk about rate of growth and development we mean that it is a solution that has had frequent academic or study publications on a regular basis over an extended period of time. This also means that the biometric solution has seen large improvements and breakthroughs in recent studies. So to summarize what we qualify rate and development as in "history" and "frequency" which, as stated, means has there been improvements or studies done and how often.

Next on the rating scale is a 3, also known as adequate. A biometric solution can only be noted as adequate based on how much improvement has been noted and for how long. In this instance an adequate solution is one where there have been some studies over a decent amount of time. This would mean that say a new form of biometric was introduced a decade ago, however, since its introduction there has been a reasonable amount of studies done to review and improve upon the existing system. Also, a 2, is rating, "fair", we give a biometric solution when it is not enough development. Using the same example, we consider a biometric solution that was introduced 10 years ago. A biometric solution can only be considered as fair when there have only been little studies done over years. This lack of studies also means that there hasn't been much improvement or many breakthroughs for this form of biometrics.

The worst possible rating that a rubric can give is a 1 = minimal. A biometric solution would only receive this rating in the instance that there is no growth and development. A system is truly minimal in this instance because it means there are no studies being done to improve and evolve the existing solution. In today's world technology continues to evolve as well as the

growing need for security, ease of use, and application of new techniques and technologies and there a need for constant improvement.

Applications to Technology

We talk of biometrics as the future of security but security has become more than a computer that we use at a desk. Telecare medical information systems are a communication between a doctor and a remote patient. We are trying to make a system secure but it is becoming more than a computer; it's becoming mobile, with new security challenges, and more diverse in applications as the technology evolves. When we talk of applications as a means of rating a biometric solution we mean that the solution has a diverse means of security implementation.

An excellent = 4 is when we see a diverse means of application for a given biometrics solution. A solution such as fingerprints can be rated as a 4 because from computers to mobile devices there is a wide selection of applications from a hardware perspective. There are diverse applications that in turn allows for a more mobile approach such as tablets and smart phones. Biometrics are being used as a way to authenticate users instead of the use of passwords.

An adequate 3 would be when there are some applications from a hardware perspective which allows a somewhat diverse approach to security authentication. A fair = 2 shows that there are little too few applications to the given biometric solution. Finally the worst rating of 1 would be that the given biometric solution has only one form of application as a means to security.

Implementation

The technology we use for biometric solutions can range from the simple mobile device for fingerprint scans to the bulky and complex devices to scan for optical biometrics. When a business implements a new technology for use as a security solution they need to take into account the cost it takes to implement it as well as effort it takes to incorporate it into the company's new or current system. That said, a business needs to take these two concepts into account when deciding which solution they wish to use for their security.

A company can use a secure solution however, if takes an astronomical amount of funding to implement it then not seen as viable means to secure the system. Also, to manage the project's schedule a business needs to also take into account the time and effort to implement the given biometric solution. We use this category as a means to rate a biometric solution in order to make the most effective decision for a security solution from a business perspective. From the least cost and effort to the most we see what makes a solution the optimal choice.

As stated in the previous rubric categories we see that a 4 of excellent is the optimal choice, however, for this category what makes a solution a 4? An excellent can only be noted by cost and effort needed in order to implement the desired biometric solution. Say a business wishes to implement a fingerprint biometric solution, they can note as a 4. Why, well there are multiple levels of complexity of fingerprint biometric solutions, however, the easiest allows for the use of mobile devices in order to accurately read a fingerprint to use as a password in order to create and authenticate a session for a Telecare medical information system. We also see from a cost perspective that there is high cost efficiency due to lack of need for expensive hardware as well as a lower need for labor which also reduces expenses. To summarize, a 4 is when there is low cost and high level of ease for implementation.

3, also known as adequate. It is when the solution is somewhat expensive to implement and there is then is difficulty when implementing the biometric solution. Say a business wishes to implement a new form of biometrics that has recently been studied and created. A business sees this biometric solution as a means to improve the security of their Telecare medical information system; however, it requires a little more effort to integrate as well as a new hardware and extra man power. As a result of this, we see that this given solution is adequate because it requires some time and effort to implement.

2 is known as a rating for fair in all levels of the rubric. In relation to cost and ease of implementation with any given biometric solution there is a need for a moderate amount of time, effort, and cost to implement. In order to integrate the given biometric it requires a fair amount of cost to integrate such as the amount of technology and labor. The given biometric solution is pricey, and from a business perspective it requires a lot of time in labor costs in order to reach a sufficient level for security implementation.

A rating of 1 minimal is noted as the worst rating a biometric solution can receive. At this level, a biometric solution is high in cost due to a high need of labor and the cost it takes integrates the hardware and other components into the system. When a business tries to implement this biometric solution it is very difficult to implement the technology and techniques, making it very difficult to produce a final working security solution. This is a rating that indicates that the biometric solution may not be the optimal choice.

User

Users are the people that would use Telecare medical information system. These users can be a doctor or a patient; however, in the end they both need to access data for personal or business use. Users transmit their personal information over public channels and therefore there is a growing need for security. As a result, biometrics are proposed as the new, more secure security solution, however, a user needs to know which biometric solution can best protect their data. As a result, there is a need for a means decide which form of security can best protect them when they use their Telecare medical information system for medical means. What makes a user make his decision is based on the biometric solutions accuracy, security, applications, and ease of use.

Table 2. User Rubric

	4 = excellent	**3 = adequate**	**2 = fair**	**1 = minimal**
Accuracy				
Privacy				
Ease of use				

Accuracy

When a user goes to input the given biometric input, how accurately this input is read is of great importance. A key component of any biometric solution is a need to accurately register, store and read a biometric input. Say a user is using a new biometric solution; first they must register an as accurate biometric input as possible to register the user. Second, the biometric solution must have a means to store as accurate an input as possible. Finally, a biometric solution must have the capability to read at every password or new session stage. These three things show the importance that accuracy has on a biometric solution

A situation where a given biometric solution can be rated from as excellent from a user stand point is when it meets all the qualifiers. A biometric solution it can only be excellent when

it highest level of accuracy due to high level of hardware and software which allows the user to register the biometric input as accurately as possible. Second, the given biometric solution must be able to store keep an as detailed and accurate biometric input as possible. Finally, the solution be able to effectively access and compare the biometrics in order to easily identify the user.

An adequate biometric solution, 3, has reasonable hardware and software to work with in conjunction with each other in order an accurate biometric. The solution can have accurate readings for the registering phase which allows a good biometric input. The biometric solution must have adequate hardware such as storage capacity in order to store a good biometric reading. Finally, a biometric solution is only truly adequate when it can compare a good stored and read biometric input in order to establish a secure session.

A fair rating of two is denoted as a modest level of accuracy given for the specific biometric solution. What this means is that the biometric solution is only somewhat accurate and may sometimes fail in authenticating a given user. This could mean many things, from faulty software which does not allow with consistent authentication to faulty hardware that does not store correct data. Three faults can be noted as bad registered input, bad data store, and finally non consistent data compare.

The final and worst rating a biometric solution can receive is a minimal 1. This type of biometric solution consistently fails to authenticate a user making the system inaccessible and the inability to create a secure session. What contributes to this failure is the inadequate hardware which can't create consistent and usable biometric inputs. A given biometric solution is also unable to safely secure an accurate biometric input. Finally, the biometric solution, due to either bad hardware or software is unable to compare and authenticate the given user.

Privacy

For any user privacy is absolutely important because it denotes whether a user can trust a system to protect sensitive data and allow a secure session between two parties over a public channel. Users need privacy and as a result, they look at biometric solutions as a new means to secure their personal info. Privacy is what allows users to know that their data is safe and others will be unable to access their data.

In this case, the rating of an excellent 4 can only be achieved when the biometric solution is not susceptible any form of attacker, hacker or any malicious individual. Also, a biometric solution must have secure input that allows for little to no ability to guess, copy, or imitate. An example of this is when a new biometric solution proposes a new unique way to replace the conventional password or other privacy authentication. A 4 would be something like a fingerprint which is hard to crack and is unique to individual.

When we encounter an adequate biometric solution, with a rating of 3, it is when there are some instances where the privacy is overcome and it results in the loss of personal information. This can mean there is some fault in the existing biometric solution, some fault that allows users to guess, copy, or imitate the user input. A user's input information may be intercepted before arriving at its destination allowing the attacker to obtain the user's input. A given biometric solution may be fair, with a rating of 2, due more frequent attacks that allow users to guess, copy, or imitate the user input. During a session is an attacker is often to gain the user input to gain access. Finally a minimal rating of 1 is when there no privacy preventing attackers from guessing, copying, or imitating the user input.

Ease of use

Ease of use refers to how easily a user can use a biometric solution. Sounds simple, however, usually complexity and security can go hand in hand. A given biometric solution may have a multi-staged process and a complex biometric input. As a result, the biometric solution could be secured better than a simple user name and password. There is a need to maintain balance of complexity and security so users can easily access a system with little to no worry over the threat to their personal information.

The optimal choice for a biometric solution would be one with one input and little too few extremely secure steps to the authentication process. Such a system can be rated as an excellent, 4, because it maintains security without the large amount of cost of an effort that comes with setting it up. A rating of 3 stands for some complexity and good security. A fair rating of 2 is when there is a moderate amount of complexity and a little difficulty to use while still remaining secure. Finally a 1 rating, minimal, is when there is a lot of complexity making it difficult to use while still being secure to the user.

Technological

This level when rating a biometric solution can be described as a rating based on how the system works from a physical standpoint. This means that when we look at a given biometric solution we are looking to see what makes the solution functional and efficient. Unlike a business and user view, we see a biometric solution through technological standpoint.

Table 3. Technological Rubric

	4 = excellent	**3 = adequate**	**2 = fair**	**1 = minimal**
Protection				
Rate of growth				
Precision				
Complexity				

Protection

For any given Telecare medical information system security is always viewed as most crucial factor. If a system is not secure the session cannot be established otherwise users private information is open for anyone to look at and use. Unlike these other views, when we look from a technological view we see that it is both the physical and technical components of a Telecare medical information system it secure. Whether it is the latest or oldest hardware or software from decades ago to today, all this can affect security.

A 4 of excellent from a technological standpoint is when a biometric solution is using the most cutting edge hardware and software. As stated before, security can also be attributed at both a physical and technical level. This means that for any given biometric solution that they are using the latest, fastest, and most efficient hardware. This also means the software and authentication process is perfected, therefore preventing any and all forms of attack. With the combination of these two things we can see from a technological standpoint that the system is secure.

A step below a 4 is an adequate biometric solution. With a rating of 3, this level of security can be described as a slightly lower quality of hardware and software. When the security is adequate, the hardware is slightly out of date and the software used is not of the latest. Without date software and an authentication process slightly lacking, this kind of biometric solution lack security. As a result of this when attacked, there are times that an attacker is able to breach security and obtain sensitive information.

Even below that would be a fair rated solution. With a rating of 2 this rating of a biometric solution has older hardware used to run the biometric security solution. Along with

that, the given biometric solution has out of date software and a pore authentication process. All of these contributing factors results in a low quality biometric solution that is susceptible to frequent attacks and security breaches. Though not the worst biometric solution, this is still an undesired level of security since it cannot always protect a user's sensitive information.

Finally the worst rating that a given biometric solution can achieve is minimal rating of 1. In the instance of a minimal biometric solution the security is almost nonexistent due to the use of out of date and no longer supported hardware. This, in combination to the same quality software, this biometric solution can't function. Also, when the authentication process is poor, an attacker has a golden opportunity to crack and access any given system.

Rate of growth and development

Not just from a business but also from a technological viewpoint is rate of growth and development important. As technology improves so does the threats to a given system due to faults in the hardware, software, and the authentication process. This sounds similar to security; however it is not dealing with the ability to fight threats but the ability to improve on existing or future faults that may exist in a given system. How fast it improves and to what level proves the ability and potential a given biometric solution may have.

The Best rating given is 4, excellent, which shows the amazing potential a given biometric has due to a high rate of growth. Any given biometric solution can only be excellent when you can find a high history of studies and reports over an extended period of time. These are results of people's hard work which show improvements to an existing system or proposals of new, more efficient hardware, software, or authentication process. As a result of high growth

and development we see its effects on other key qualities such as accuracy, surety, and complexity.

A biometric solution achieves a 3 when we see a lower rate of growth and development. This means that the given biometric over the same time frame has shown less amounts of studies and reports on a given biometric solution. This decrease in growth can result lack of improvements on a system that eventually encounters the threats of attackers. On the other hand a fair rating of 2 is when there barely any growth at all. This means when a give Telecare medical information system faces a threat of attackers due to a flaw in a systems security or authentication process a may take a long time for improvement.

When a given biometric solution achieves a rating of minimal = 1 it means that there is little to no growth. Without growth there is no hope, because every day the threat of security grows. Attackers are always trying to get personal private information and as a result they constantly improving their techniques and technologies in order to achieve their goals. In order to prevent this from happening there is an ongoing a need for growth.

Precision

Precision is of key importance when it comes to any biometric solution. Precision from the hardware and software are what makes the authentication process feasible and also relates to how complex and costly a given security solution is. With a fingerprint biometric solution as an example it can either be cheap and simple, possibly at the cost of precision, or pricey and complex, however, accurate. Finally the authentication process can be attributed to precision because at the registration phase, if an inaccurate biometric signature is taken it may not be able to complete authentication.

A 4 is when a highly accurate system has an accurate biometric solution. This means that that the registration phase the level of hardware and software that allows a readable and easy to compare biometric input. This accurate input is then stored for use later on at the authentication phase in order to initiate a secure session. When a system has few inaccurate inputs it is then noted as an adequate solution. As a result of this level of precision there are some instances of inaccurate registration that then results in failed authentication.

When there are few accurate inputs it is then noted as a fair solution. As a result of this level of precision there are many instances of inaccurate registration that then results in failed authentication. The worst rating of precision when there are little to no instances of accurate inputs it is then noted as a minimal solution. As a result of this level of precision there are little to no instances of accurate registration that then results in failed authentication.

Complexity

Complexity is a crucial factor when looking to implement new security into a system. With a rise in complexity comes a rise in labor, money, and time. Also, complexity can attribute to a higher difficulty when implementing a new solution. That said, complexity always needs to be taken into account with any new system. Complexity is what effects not only implementation of a solution but also its uses and its effectiveness.

When we look at an excellent solution there is little to no complexity. A 4 also means that as a result of a lack in complexity there is a decrease in cost, labor, and time. This is the optimal solution when implement any new biometric solution into a Telecare medical information system. Finally, a lack of complexity can also result in an easier effort of implementation and design.

A step below an excellent would be an adequate solution. Rated as a 3, this level of complexity is denoted as having some complexity. As a result of this, there is a little increase in cost, labor and time. This level of complexity also means a higher need of effort when implementing the solution. A 2 on the other, has a high level of complexity resulting in a more significant increase in cost, labor and time. This level of complexity also means a high need of effort when implementing the solution.

The lowest rating would be a minimal rating of 1. This level of complexity is extreme making the solution as complex as it can be. When we look at this kind of biometric solution, we see a costly effort that also requires a high level of labor in order to be properly implemented. Due to the amount of complexity there is a need for lots of extra effort over a large extended period of time. The final result is a biometric solution that is implemented over a long pricey effort or one that may not be even implemented at all due to its complexity.

CHAPTER 5 ANALYSIS: WHAT IS TRULY SECURE?

Below is the master table of all examples given for this chapter:

Table 4. Master example table

Example Number	Description
Ex. 1	Practical chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices e.g. cell phone and PDA.
Ex. 2	A novel fingerprint template protection scheme based on chaotic encryption by using the logistic map and Murillo-Escobar's algorithms
Ex. 3	This encryption algorithm is constructed with four chaotic systems, which consist of two 1-D and two high-dimensional 3-D chaotic systems.
Ex. 4	Visible iris recognition using deep sparse filtering.
Ex. 5	Iris liveness detection for mobile devices based on local descriptors.
Ex. 6	Video-based signature verification and pen-grasping posture analysis.
Ex. 7	On-line signature verification using multiresolution feature extraction and selection.

Fingerprint Pattern

We have already taken a look at the structure of what we define truly makes a biometric solution the proper choice. By defining key attributes of a multi-dimensional view of security solutions we can then properly analyze and rate any given biometric solution. In order to better understands a given solutions pros and cons we must use a refined system in order to effectively decide on a final solution. The goal of this thesis is to research and better understand what makes a biometric solution the best for a TMIS or any other system that needs better security.

We first look at the fingerprint. The fingerprint is a unique form of physical biometrics. With biometrics, physical biometrics is a biometric that is based on a physical trait of an individual versus its counterpart the behavioral biometric such as a signature. By looking at three distinct versions of fingerprint biometrics we hope to see some pattern, if not strengths and weaknesses to the given categories. By doing this, we are then able to effectively decide why or

why not to choose a form of fingerprint biometric security. We have already defined and described what fingerprint biometrics are and we now look at chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices as an example of such an implementation. Fingerprint biometrics is more than just using a scanned print as a password, it is also part of a distinct process that stores these prints in a given security structure. With Chaotic hash-based fingerprint:

> A hash function is a one-way transformation that takes an arbitrary input and returns a fixed-size string, named as hash value or message digest. Recent work on collision frequencies reveals many undiscovered flaws in conventional cryptographic hash algorithms, and it is still a challenging open problem for further study of secure hash function. ….. Utilizing some interesting characteristics of chaos, such as the sensitivity to initial condition and control parameter, ergodicity and mixing property, a chaotic hash algorithm was constructed in, which is based on an n-D nonlinear autoregressive filter. The iteration process of chaotic systems is one-way, which make them an ideal candidate to be used for the collision free one-way hash functions. Combined the properties of chaos with cipher block chaining (CBC) mode in hashing process, the chaotic hash function can meet the requirements of cryptographic hash, though its further security analysis is very necessary for a reliable security system. (Khurram, Zhang, and Wang, 2008)

That said, with the combination of a one way hash function and the authentication scheme we see a combination of biometrics through the use of mobile devices. By properly evaluating the proposed schema through the use of the thesis proposed multi-dimensional rubric

we can see whether or not the proposed biometric solution if we wanted to used it for a TMIS system.

Table 5. Fingerprint rate example

Business	**Ex. 1**
Security	4
Development	3
Applications to Technology	4
Costs and ease of implementation	3
SUBTOTAL	14
User	
Accuracy	4
Privacy	3
Ease of use	4
SUBTOTAL	11
Technological	
Protection	3
Rate of growth and development	3
Precision	3
Complexity	4
SUBTOTAL	13
TOTAL	38

Titled *A robust embedded biometric authentication system based on fingerprint and chaotic encryption* this is another interesting fingerprint biometric proposal. In this case, fingerprint biometrics are used to "present a novel fingerprint template protection scheme based on chaotic encryption by using the logistic map and Murillo-Escobar's algorithm (Murillo-Escobar et al., 2014). In addition, we present a novel implementation of our scheme in a 32 bit microcontroller for secure authentication systems to show its application on embedded expert systems." (Murillo-Escobar, M.a., Cruz-Hernández, Abundiz-Pérez, and López-Gutiérrez, 2015) Through the use of encryption they use an algorithm previously proposed as Murillo-Escobar's algorithm as a means to safely encrypt a user's biometric signature in order to create a secure connection.

Table 6. Fingerprint rate example 2.

Business	**Ex. 1**	**Ex. 2**
Security	4	4
Development	3	4
Applications to Technology	4	4
Costs and ease of implementation	3	3
SUBTOTAL	14	15
User		
Accuracy	4	3
Privacy	3	4
Ease of use	4	4
SUBTOTAL	11	11
Technological		
Protection	3	3
Rate of growth and development	4	2
Precision	3	3
Complexity	4	2
SUBTOTAL	14	10
TOTAL	39	36

This example presents "a new multiple chaos-based biometric image cryptosystem for fingerprint security. This encryption algorithm is constructed with four chaotic systems, which consist of two 1-D and two high-dimensional 3-D chaotic systems. This algorithm enhances the security strength of biometric image cryptography that incorporates single chaos and multiple 1-D chaotic systems." (Murillo-Escobar, M.a., Cruz-Hernández, Abundiz-Pérez, and López-Gutiérrez, 2015) This proposal shows a different approach to fingerprint biometrics through the use of four distinct chaotic systems:

The fingerprint image encryption algorithm is designed with the four chaotic systems serving the following functions

1. Logistic map is served as the adjusted initial value generator.
2. HULA is utilized to scramble the pixels' positions of fingerprint image.
3. Chebyshev map is used as the encrypted key generator.

4. APFM nonlinear adaptive filter is employed to generate the dynamic substitution box (S- box). (Murillo-Escobar, M.a., Cruz-Hernández, Abundiz-Pérez, and López-Gutiérrez, 2015)

Below is the final comparison of the first two examples to this new proposed biometric solution

Table 7. Fingerprint rate example 3

Business	**Ex. 1**	**Ex. 2**	**Ex. 3**
Security	4	4	4
Development	3	4	3
Applications to Technology	4	4	3
Costs and ease of implementation	3	3	2
SUBTOTAL	14	15	12
User			
Accuracy	4	3	4
Privacy	3	4	3
Ease of use	4	4	4
SUBTOTAL	11	11	11
Technological			
Protection	3	3	3
Rate of growth and development	4	2	3
Precision	3	3	3
Complexity	4	2	2
SUBTOTAL	14	10	11
TOTAL	39	36	36

Ocular Pattern

The eyes are another prominent form of physical biometrics. Unlike the fingerprint however, the eye is split up into a few distinct form of biometrics such as the iris and ocular region with the most prominent being the iris. We now look at three distinct forms of ocular biometrics solutions in order to better understand the pros and cons of this medium of biometrics as well as what makes it a good choice when implementing a TMIS security solution. Below are three distinct forms of ocular biometric solutions.

One form of Ocular biometrics is through using the iris in conjunction with "Recent works have identified visible spectrum iris recognition as a viable option with considerable

performance. Key advantages of visible spectrum iris recognition include the possibility of iris imaging in on-the-move and at-a-distance scenarios as compared to fixed range imaging in near-infra-red light (Raja, Kiran B., Raghavendra, Vemuri, and Busch, 2015) Through this we adapt it to work "we propose a new segmentation scheme and adapt it to smart phone based visible iris images for approximating the radius of the iris to achieve robust segmentation." (Raja, Kiran B., Raghavendra, Vemuri, and Busch, 2015) Like other forms of security, the smartphone is continuing to be growing in importance in relation to security due to its ease of use, applications and mobility.

Results already show that the proposed technique "has shown the improved segmentation accuracy up to 85% with standard OSIRISv4.1."(Raja, Kiran B., Raghavendra, Vemuri, and Busch, 2015) However, unlike other smart phone based techniques, "this method uses proposes a new feature extraction method based on *deep sparse filtering* to obtain robust features for unconstrained iris images. To evaluate the proposed segmentation scheme and feature extraction scheme, we employ a publicly available database and also compose a new iris image database."(Raja, Kiran B., Raghavendra, Vemuri, and Busch, 2015) With these unique features we look at this technique as a whole to better understand based on the proposed rubrics show the pros and cons to this new method.

Table 8. Ocular rate example

Business	**Ex. 4**
Security	4
Development	4
Applications to Technology	4
Costs and ease of implementation	4
SUBTOTAL	16
User	
Accuracy	4
Privacy	4
Ease of use	4
SUBTOTAL	12
Technological	
Protection	4
Rate of growth and development	4
Precision	4
Complexity	4
SUBTOTAL	16
TOTAL	44

Iris recognition is the most prominent means of ocular biometrics, however, it still faces instances where when used as a security control it is insecure. The studies we look at show improvements and proposals on new techniques and scheme in order to better guarantee adequate protection. For a security solution for TMIS iris biometrics is a great choice for security. The second example of ocular biometrics is Iris liveness detection for mobile devices. Unlike the sparse filtering of the first example this solution "looks to improve and prevent authentication systems from being easily tricked by attacks based on high-quality printing."(Gragnaniello, Diego, Sansone, and Verdoliva, 2015)

In order to prevent high-quality printing "A liveness detection module is therefore necessary. Here, we propose a fast and accurate technique to detect printed iris attacks based on the local binary pattern (LBP) descriptor. In order to improve the discrimination ability of LBP and better explore the image statistics, LBP is performed on a high pass version of the image

with 3×3 integer kernel."(Gragnaniello, Diego, Sansone, and Verdoliva, 2015) The rubric below denotes the rating for the given example:

Table 9. Ocular rate example 2

Business	**Ex. 4**	**Ex. 5**
Security	4	4
Development	4	4
Applications to Technology	4	4
Costs and ease of implementation	4	3
SUBTOTAL	16	15
User		
Accuracy	4	4
Privacy	3	3
Ease of use	4	4
SUBTOTAL	12	12
Technological		
Protection	4	4
Rate of growth and development	4	4
Precision	4	4
Complexity	4	4
SUBTOTAL	16	16
TOTAL	43	42

Signature Pattern

A signature is categorized as a form of behavioral biometrics. Behavioral biometrics is the measure of uniquely identifying and measuring patterns specifically related to human activities such as voice or signature. Like the other forms of biometrics, signature also has its pros and cons compared to other forms of biometrics. By taking a closer look and distinct examples of biometrics we are able to understand whether or not a signature is a viable means of security. Below are three distinct forms of signature biometric solutions.

One unique signature biometric solution is Video-based signature verification and pen-grasping posture analysis for user-dependent identification authentication. With this form of biometrics comes the proposal of "a video-based identification authentication framework via signature verification and pen-grasping posture analysis. The authors consider the case of using a

camera instead of a pressure-sensitive tablet to acquire signatures. The proposed reliable verification method is useful when pressure-sensitive digitizing tablets are not available" (Cheng, H.-Y., Yu, Gau, and C.-L. Lin, 2012).

Unlike traditional forms of signature biometrics, this new method allows for acquiring additional information besides the trajectories of the signature. Unlike a fingerprint,

> The entire writing process and the pen-grasping posture are personalized features that cannot be easily imitated and forged. The authors analyze the signature trajectories using curvelets and the pen-grasping posture using modified motion energy images to perform user-dependent identification authentication. The proposed system is able to achieve both low false-rejection rates and low false-acceptance rates for database containing both unskilled and skilled imitation signatures. (Cheng, H.-Y., Yu, Gau, and C.-L. Lin, 2012).

This allows for a more accurate and reliable signature.

Table 10. Signature rate example

Business	**Ex. 6**
Security	4
Development	4
Applications to Technology	2
Costs and ease of implementation	2
SUBTOTAL	12
User	
Accuracy	4
Privacy	3
Ease of use	4
SUBTOTAL	11
Technological	
Protection	3
Rate of growth and development	4
Precision	4
Complexity	2
SUBTOTAL	13
TOTAL	36

Handwritten signatures are a common behavioral biometric. With this biometric solution they proposed the idea of new features.

> The main challenge of signature verification is the high dimensionality of the signature features dataset that makes the corroboration procedure computationally costly. In this example paper, they reduced the dimension of the input data with almost no loss of information. To this end, wavelet transform and fusion techniques were used to propose a new set of features. In addition, we introduced an effective feature selection technique, which was based on applying a filter box to find the most informative parts of the data and eliminate redundancies. (Nilchiyan, Reza, and Yusof, 2014)

The result of these methods was an improvement on operating speeds and a reduction on memory usage. They even managed to obtain an Equal Error Ratio (EER) of 2.5%, with considerably fewer features.

Table 11. Signature rate example 2

Business	**Ex. 6**	**Ex. 7**
Security	4	4.
Development	4	4.
Applications to Technology	2	2
Costs and ease of implementation	2	2
SUBTOTAL	12	12
User		
Accuracy	4	3
Privacy	3	3
Ease of use	4	4
SUBTOTAL	11	10
Technological		
Protection	3	3
Rate of growth and development	4	3
Precision	4	4
Complexity	2	2
SUBTOTAL	13	12
TOTAL	36	34

The study shows that a signature with more features does not necessarily result in higher performance. This is all due to the need for more hardware such as memory and processing. This also requires more signatures provided by the signer to be able to train the verification system. The system needs to be able to identify these features in order to better identify false from true signatures.

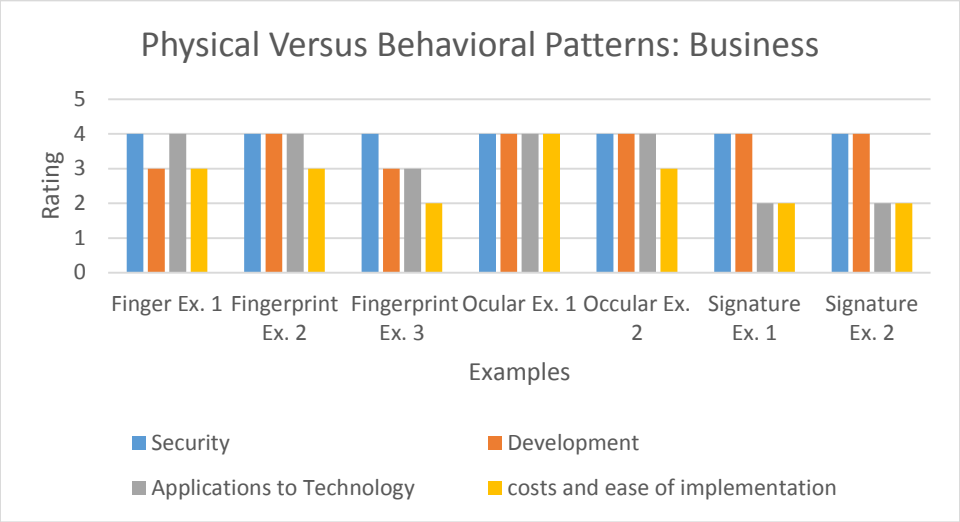
Vocal Pattern

Voice biometrics is also another form of behavioral biometrics that can also be used for TMIS security solutions. There are many journals and articles that go into detail about the applications of voice biometrics. The FBI has even done extensive research on "Speaker, or voice, recognition is a biometric modality that uses an individual's voice for recognition purposes. (It is a different technology than "speech recognition", which recognizes words as they are articulated, which is not a biometric.) The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual." (FBI)

Patterns Found in Biometric Solutions: Business

With any given security there is definitely some form of pros and cons. The point of this thesis is to use the generated rubrics in order to see these pros and cons of any given biometric solution. Each form of biometric is unique and we have already stated the difference between both behavioral and physical biometrics. By comparing results between multiple types of biometric solutions we can better understand how the rubrics are used as well as see how biometrics rate. The chart below denotes how both fingerprints and eyes can be rated using the business rubric.

Figure 1. Trait Comparison: Business

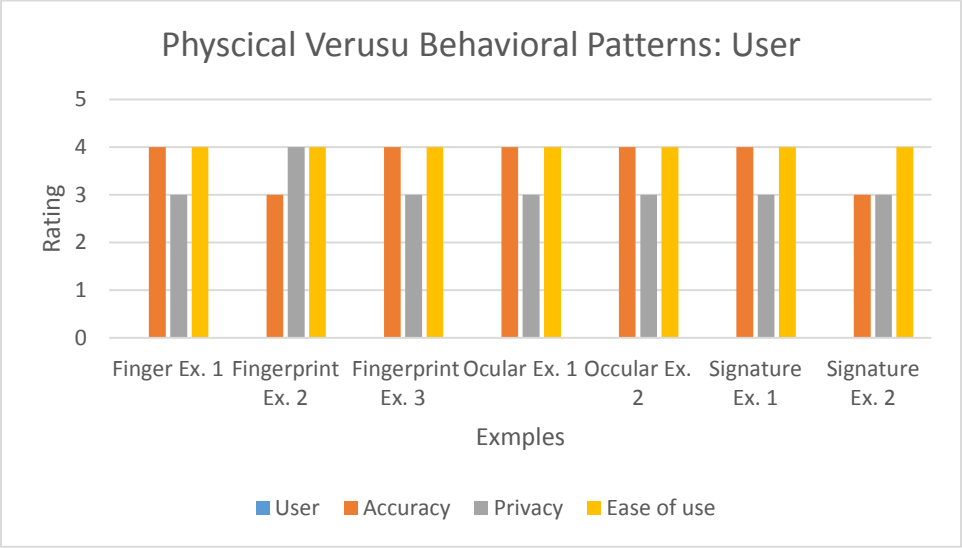


The above chart shows that for physical biometrics these two types of biometrics are very similar. When it comes from a business standpoint, for most examples security and Applications to technology is rated highly. This in turn shows that physical biometrics are secure and have multiple means to apply their given technologies and techniques. On the other hand, the cost and ease of implementation and development, though not perfect, also seems to be rated highly. From all this, we can gather that physical biometrics are most often a reasonable choice for a biometric solution.

On the other hand, is signature which is a form of behavioral biometrics. Like the physical biometrics, the signature is secure and also has a high rate of development. In the other hand, a signature has a low rating of applications to technology meaning that it is not very diverse for its technology modems. Finally, a signature, though secure, is costly to implement and harder to put into practice.

Patterns Found in Biometric Solutions: User

Figure 2. Trait Comparison: User

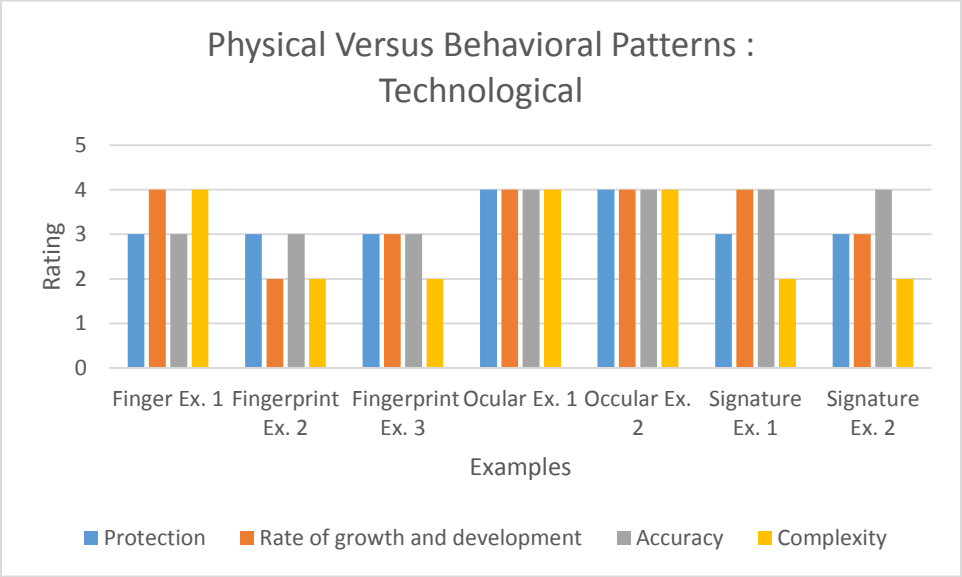


The above chart shows physical biometrics these two types of biometrics. When it comes from a user standpoint, for most examples accuracy and ease of use is rated highly. This in turn shows that physical biometrics are very accurate for registration as well as the login phase. Ease of use means that any person no matter what level of education or background can easily use on their first time as well as every successive one. On the other hand, the privacy, though not perfect, also seems to be rated highly. From all this, we can gather that physical biometrics are a great choice for a biometric solution.

When compared with physical biometrics we see some minor discrepancies in comparison. A signature has a high rating of ease of use meaning that it is also very easy to use for most users. Privacy unlike security means that information is not exposed to prying eyes. Like physical biometrics, a signature hovers around a rating of 4 or 3 for how well it maintains privacy. Finally, a signature also tends to have a higher rating of accuracy showing that the hardware and software in place allows for few instances of failure when reading a user's input.

Patterns Found in Biometric Solutions: Technological

Figure 3. Trait Comparison: Technological



A technological view means that we rate a biometric solution by understanding the technical aspects of a given biometric solution. They can be the system as a whole or the hardware and software that makes them. From the physical biometrics we see that a fingerprint biometric has more often or not a mid to low level reading for protection, rate of growth and development, accuracy and complexity. For eyes however, we see that across the board, it is a form of biometrics that is solid in all aspects of the technological rubric.

With behavioral biometrics we see a mix of ratings for a technological viewpoint. A signature has higher precision in comparison to fingerprint biometrics, however, it is different for the other categories. When we look at complexity we see that the signature has a low rating which signifies a high level of complexity in the system. On the other hand, we see that there is a similar rating for all the solutions when it comes to protection and rate of growth and development.

CHAPTER 6 CONCLUSION

The results of this study show the effectiveness of using a rubric as an effective means for selecting future biometric security solutions. A business that is selecting a prospective security solution can in turn go through the three dimensional rubric in order to get a multi-facet view from a user, business, and technological standpoint. With this rubric, a business can see not only the pros of a biometric solution but also the cons. A form of signature biometrics may rate highly from a business standpoint, however, that may not be the case from a user standpoint. This in turn brings to life the idea of the use of multi-modal biometrics

Multimodal means that a security solution would be a combination of different forms of biometrics. This all done in order to make up for the weaknesses for different forms of biometrics in order to make a more secure solution. Many studies in recent years, such as *BIOMETRICS IN HEALTH CARE SECURITY SYSTEM IRIS-FACE FUSION SYSTEM*, start to show this new practice of security and it seems to be more effective. In this instance we can see the benefits of fusion of both iris and face recognition. As a result, this may prove to be a viable solution for TMIS.

REFERENCES

Biometrics. (n.d.). *Dictionary.com Unabridged*. Retrieved March 03, 2016 from Dictionary.com websitehttp://dictionary.reference.com/browse/biometrics

Cheng, H.-Y., C.-C. Yu, V. Gau, and C.-L. Lin. "Video-based Signature Verification and Pen-grasping Posture Analysis for User-dependent Identification Authentication." *IET Computer Vision* 6.5 (2012): 388-96.

Debiao, He, Chen Jianhua, and Zhang Rui. "A More Secure Authentication Scheme for Telecare Medicine Information Systems." *J Med Syst Journal of Medical Systems* (2011): 1989-995.

Doroz, Rafal, Piotr Porwik, and Tomasz Orczyk. "Dynamic Signature Verification Method Based on Association of Features with Similarity Measures." *Neurocomputing* (2015): 921-31.

Galbally, Javier, Moises Diaz-Cabrera, Miguel A. Ferrer, Marta Gomez-Barrero, Aythami Morales, and Julian Fierrez. "On-line Signature Recognition through the Combination of Real Dynamic Data and Synthetically Generated Static Data." *Pattern Recognition* (2015): 2921-934.

Guo, C., & Chang, C. (2013). Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation, 1433-1440.

Gragnaniello, Diego, Carlo Sansone, and Luisa Verdoliva. "Iris Liveness Detection for Mobile Devices Based on Local Descriptors." *Pattern Recognition Letters* 57 (2015): 81-87.

Guo, D., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2015). A Novel Authentication Scheme Using Self-certified Public Keys for Telecare Medical Information Systems. J Med Syst Journal of Medical Systems.

Khalil, M., Kurniawan, F., & Saleem, K. (2013). Authentication Of Fingerprint biometrics Acquired Using A Cellphone Camera: A Review. *Int. J. Wavelets Multiresolut Inf. Process. International Journal of Wavelets, Multiresolution and Information Processing*, 1350033-1350033.

Khan, Muhammad Khurram, Jiashu Zhang, and Xiaomin Wang. "Chaotic Hash-based Fingerprint Biometric Remote User Authentication Scheme on Mobile Devices." *Chaos, Solitons & Fractals* 35.3 (2008): 519-24.

Khitrov, Mikhail. "Talking Passwords: Voice biometrics for Data Access and Security." *Biometric Technology Today*: 9-11.

Kumar, A., & Kwong, C. (2015). Towards Contactless, Low-Cost and Accurate 3D Fingerprint Identification. *2013 IEEE Conference on Computer Vision and Pattern Recognition*.

Leng, Xuefei. "Smart Card Applications and Security." *Information Security Technical Report* (2009): 36-45.

Markowitz, Judith A. "Voice biometrics." *Communications of the ACM Commun. ACM* (2000): 66-73.

Mishra, Dheerendra. "Understanding Security Failures of Two Authentication and Key Agreement Schemes for Telecare Medicine Information Systems." *J Med Syst Journal of Medical Systems* (2015).

Murillo-Escobar, M.a., C. Cruz-Hernández, F. Abundiz-Pérez, and R.m. López-Gutiérrez. "A Robust Embedded Biometric Authentication System Based on Fingerprint and Chaotic Encryption." *Expert Systems with Applications* 42.21 (2015): 8198-211.

Nilchiyan, Mohammad Reza, and Rubiyah Bte Yusof. "On-Line Signature Verification Using Multiresolution Feature Extraction And Selection." *International Journal of Pattern Recognition and Artificial Intelligence Int. J. Patt. Recogn. Artif. Intell.* 28.03 (2014): 1456005.

Nigam, I., Vatsa, M., & Singh, R. (2015). Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, 1-35.

Raja, Kiran B., R. Raghavendra, Vinay Krishna Vemuri, and Christoph Busch. "Smartphone Based Visible Iris Recognition Using Deep Sparse Filtering." *Pattern Recognition Letters* 57 (2015): 33-42.

"Voice Recognition." *FBI*. FBI, 29 Jan. 2013. Web. 3 Jan. 2016.

Xie, Q., Hu, B., Dong, N., & Wong, D. (2014). Anonymous Three-Party Password-Authenticated Key Exchange Scheme for Telecare Medical Information Systems. PLoS ONE.

Wu, Fan, and Lili Xu. "Security Analysis and Improvement of a Privacy Authentication Scheme for Telecare Medical Information Systems." *J Med Syst Journal of Medical Systems* (2013).

Wu, Z., Lee, Y., Lai, F., Lee, H., & Chung, Y. (2010). A Secure Authentication Scheme for Telecare Medicine Information Systems. *J Med Syst Journal of Medical Systems, 36*(3), 1529-1535.

Zhang, L., & Zhu, S. (2015). Robust ECC-based Authenticated Key Agreement Scheme with Privacy Protection for Telecare Medicine Information Systems. *J Med Syst Journal of Medical Systems*.