Continuous and Secure Monitoring of Biometric Sensors in Distributed Environments

Theodoros Kampouris

Master of Science

T.E.I. of Larissa

Staffordshire University

Technological Educational Institute of Larissa

May 2011

Technological Educational Institute of Larissa

Continuous and Secure Monitoring of Biometric Sensors in Distributed Environments

Theodoros Kampouris

Master of Science, 2011

Thesis Summary

The main goal of this thesis is to implement a continuous and secure monitoring of biometric sensors in distributed environments and also to help in understand the use of biometrics, the authentication methods used, the security issues regarding the sensors that collect the biometric data and some basics about cryptography.

Keywords: biometrics, authentication, security, monitoring

Contents

1 Introduction **7**
- 1.1 Introduction . . . 7
- 1.2 Aims of the Thesis . . . 11
- 1.3 Research Methodology . . . 11
  - 1.3.1 Literature Review . . . 11
  - 1.3.2 Analysis and Investigation . . . 12
  - 1.3.3 Prototyping . . . 12
  - 1.3.4 System Evaluation . . . 12
- 1.4 Novel Features of the Thesis . . . 13
- 1.5 Outline of the Thesis . . . 13

2 Cryptography **14**
- 2.1 Cryptography . . . 14
- 2.2 Goals of Cryptosystems . . . 16
- 2.3 Methods of Encryption . . . 17
  - 2.3.1 Symmetric Cryptography . . . 17
  - 2.3.2 Asymmetric Cryptography . . . 20
- 2.4 DES . . . 22
  - 2.4.1 DES Modes of Operation . . . 22
  - 2.4.2 Triple DES (3DES) . . . 24
  - 2.4.3 Triple-DES Encryption/Decryption Process . . . 24
- 2.5 Advanced Encryption Standard (AES) . . . 25
- 2.6 Cryptographic Hash Functions . . . 26
  - 2.6.1 One-way hash function (OWHF) . . . 26
  - 2.6.2 Collision resistant hash function (CRHF) . . . 27
- 2.7 Digital Signatures . . . 28
  - 2.7.1 The Digital Signature Standard (DSS) . . . 28

3 Biometric Sensors **30**
- 3.1 Biometric Identification Process . . . 30
  - 3.1.1 Acquisition of Biometric Samples . . . 31
  - 3.1.2 Storage of Biometric Templates . . . 31
  - 3.1.3 Matching/Authentication Process . . . 32
- 3.2 Success Factors for Biometrics . . . 32
- 3.3 Verification, Identification, Screening . . . 36
  - 3.3.1 Verification . . . 36

3.3.2 Identification . . . 37
3.3.3 Screening . . . 37
3.4 Advantages and Disadvantages of biometric authentication systems . . . 38
3.4.1 Advantages . . . 38
3.4.2 Disadvantages . . . 39
3.5 The Security Problem in Biometric Systems . . . 40
3.5.1 Attacks on Biometric Systems . . . 41
3.5.2 Errors on Biometric Systems . . . 42
3.6 Social, Economic, Legal and Technical Issues . . . 42
3.6.1 Social . . . 43
3.6.2 Economic . . . 44
3.6.3 Legal . . . 44
3.6.4 Technical . . . 45
3.7 Medical Aspects of Biometrics . . . 46
3.7.1 Direct Medical Implications . . . 46
3.7.2 Indirect Medical Implications . . . 47
3.7.3 IMI from DNA . . . 49
3.8 Biometrics History . . . 49
3.9 Related Ethics Issues . . . 52

4 System Design and Implementation **55**
4.1 Implementation Details . . . 55
4.2 Security . . . 60
4.3 Results . . . 62

5 Conclusions **64**
5.1 Aims of the Thesis . . . 64
5.2 Evaluation . . . 64
5.2.1 Thesis Development . . . 64
5.2.2 Proposed System . . . 65
5.3 Recommendations for Future Research . . . 65
5.4 Conclusions . . . 65

Bibliography **67**

List of Figures

2.1 The process of encryption and decryption. 14
2.2 The role of the key in the encryption process. 15

3.1 CER and Error Rate Relationship. 33
3.2 Biometric Authentication Process. 34

4.1 High-level architecture of developed system. 56
4.2 Visual display of the sensors. 57
4.3 Monitoring Client. 58
4.4 Alerts List. 59
4.5 Monitoring Graph. 60
4.6 Sensor Listener. 62
4.7 Maximum response time/Sensors system can tolerate. 63

List of Tables

2.1 AES vs Triple-DES. 26

3.1 Biometrics history. 51

Chapter 1

Introduction

1.1 Introduction

A biometric is a physical or biological feature or attribute that can be measured. It can be used as a means for either proving that you are who you claim to be, or for proving without revealing your identity that you have a certain right, just like a PIN (Personal Identification Number) or a password. The crucial difference is that the biometric is something that is part of you, rather than something you know or can carry with you. The main difference of biometrics from other digital identifiers, (like passwords, PINs or credit cards) is that biometrics cannot be lost or forgotten since biometric measurements are part of the body and as a result they will always be present when needed (European Commission JRC 2005). There are many types of biometrics like:

- **Fingerprints**: The patterns of friction ridges and valleys on fingertips are unique for every person (even for identical twins). One of the most common biometric technologies are fingerprint recognition devices. With these devices, users no longer need to remember and type passwords because a single touch provides instant access. Fingerprint systems can also be used in identification mode. For example several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names.

- **Face Recognition**: The identification of a person can also be achieved by their facial image. By capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission a person's identity can be verified. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Detecting a mask or photograph is one of the challenges of facial recognition. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Some of the benefits that facial recognition has are:
  - non-intrusive
  - hands-free
  - continuous
  - accepted by most users
- **Voice Recognition**: Voice recognition has a history dating several decades back, when the output of several analog filters was averaged over time for matching. Voice recognition uses the acoustic features of speech that have been found to differ between every person. These acoustic patterns show anatomy (like the size and the shape of throat and mouth) and also some learned behavioural patterns (like voice pitch and speaking style). Voice recognition is classified as a "behavioural biometric" because of the learned patterns into the voice templates. Voice recognition systems use three styles of spoken input:
  - Text-dependent: it is the most used style and it involves selection and enrollment of one or more voice passwords.
  - Text-prompted: this style is used when there is possibility of imposters.
  - Text-independent

Voice recognition systems have to overcome some challenges like the fact that voice changes due to aging also need to be addressed by recognition systems. These systems need some additional hardware by using existing microphones and voice-transmission technology which allows recognition over long distances via ordinary telephones.

- **Iris Recognition**: These systems use the iris of the eye which is the coloured area around the pupil and which is unique for every individual. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for many years and their cost decreases constantly. These systems can be applied and operate well in both verification and identification modes. Current systems can be used even in the presence of eyeglasses and contact lenses and there is no problem for different ethnic groups and nationalities (Podio & Dunn n.d.).

- **Retina Recognition**: Retina recognition is a technology which captures and analyses the patterns of blood vessels on the thin nerve on the back of the eye-ball that processes light entering through the pupil. Retinal patterns are highly distinctive and unique characteristics as every eye has its own totally unique pattern of blood vessels. Even if every retina normally remains unchanged over the years, it can be affected by diseases such as glaucoma, diabetes, high blood pressure or autoimmune deficiency syndrome. The fact that the retina is small, internal, and that it can't be easily to measure makes capturing its image more difficult than most biometric technologies. An individual must position its eye very close to the lens of the retina-scan sensor, stare directly into the lens, and remain perfectly still while focusing on a revolving light while a small camera scans the retina through the pupil. Any movement can interfere with the process and can require restarting. It is easy to understand that in this case enrollment may last longer than with other systems and it can easily take more than a minute (Rhodes 2003).

- **Hand and Finger Geometry Recognition**: To achieve personal authentication through hand recognition, systems measure either physical characteristics of the fingers or the hand (like length, width, thickness and surface area of the hand). Hand geometry has gained acceptance in many applications and it can be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

- **Signature Verification**: This technology uses the dynamic analysis of a signature to authenticate a person by measuring speed, pressure and angle used by the person when a signature is produced. This technology has been employed in e-business applications and other applications where signature is an accepted method of personal authentication (Podio & Dunn n.d.).

  Authentication is the mechanism which allows systems to securely identify their users. Authentication systems give answers to questions like who is the user and if the user really is who he "claims" to be.

  An authentication system may be simple, and as a result more insecure (like a plain- text password challenging system) more complicated (like the Kerberos system) and also token-based authentication systems (which authenticate users holding the token.

  Tokens could be smart cards without any pin requests, RFID tags, magnetic keys and many more). In any case, authentication systems depend on some unique bit of information which is known only to the user being authenticated and the authentication system. Such information may be a typical password, some biometric characteristics of the individual (like fingerprints, iris or voice recognition etc.), or some derived data (like smartcard systems). In order for a user to be identified by a system, the authenticating system typically challenges the user to provide his unique information to it and if the authenticating system can verify that this information was presented correctly, then the user is considered authenticated (Duke University n.d.).

Authentication systems based on biometrics operate by processing the data being sent by sensors assuming that the data are secured and the sensor haven't been "fooled" in any way. So apart from the authentication we need to be sure that the data being authenticated are original and that the authentication process will authenticate the right user. The goal is to eliminate cases where the authentication of a user is successful and despite that the system might have granted permission and authorities to the wrong person.

Authentication systems based on biometric characteristics are considered to be more secure than others as biometrics cannot be stolen because they are part of the person being authenticated. Systems would be even safer if there was a way to monitor the biometric-sensors and be somehow certain that they are working properly at all times. The creation of an application that can do this is the main concern and motivation of this thesis.

1.2 Aims of the Thesis

1. Aim of this thesis is at first to present a survey on biometrics and sensors which collect biometric characteristics and the security issues that may arise in networks operating based on biometric authentication systems.

2. The second aim is the implementation of an application that securely monitors a distributed network of biometric sensors and immunises a safe communication between sensors and a central server.

1.3 Research Methodology

1.3.1 Literature Review

In order to complete this thesis several things will be needed:

- A good understanding of cryptography as a general meaning and more specific a good understanding of the several existing cryptographic algorithms.
- A good understanding of biometrics and the way that systems based on biometric authentication systems operate.
- The application should be implemented in a programming language that will be platform independent and that will support distributed environments.

1.3.2 Analysis and Investigation

First of all a deep survey in authentication systems based on biometric characteristics and in biometrics in general is necessary in order to present them in the best possible way. Also a survey in cryptography and the several cryptographic algorithms will be needed so as to present the importance of cryptography and decide what the best cryptographic algorithm is to use it for the application that will be developed. At last there must be decided a programming language for the development of the application that supports distributed environments and that is platform independent.

1.3.3 Prototyping

The application that will be developed will have to be in order to monitor at all times the biometric sensors that we want to monitor. The application must be robust and not vulnerable to every aspiring attacker and for that reason any communication the sensors will have with the central server will have to be encrypted. Also the application will have to be "smart" and give the opportunity to the responsible for the sensors-network to monitor it no matter where he is.

1.3.4 System Evaluation

The most important goal is to create an efficient and secure application for secure monitoring of biometric sensors that will able to detect possible attacks it may suffer.

In order for this application to be reliable the communication between sensors and the server in the application should be encrypted.

1.4 Novel Features of the Thesis

In the development of the application new ways of architectural view were used. There were used web services and management of data with the use of xml files.

Web services give the ability of access from everywhere. They send the data through "XML SOAP ENVELOPES" and they give the opportunity of reading them through several clients like laptops or even smart phones.

1.5 Outline of the Thesis

The thesis is organised as follows: Chapter 2 is all about cryptography. It gives some general information about cryptography, the goals of cryptosystems and digital signatures. It also states the several methods of encryption and explains the DES, Triple DES and AES cryptographic algorithms. Chapter 3 is a survey in biometric sensors. Here is a description of the biometric identification process, the success factors for biometrics, advantages and disadvantages and many other issues regarding biometrics. Chapter 4 describes the design of the java application and the security measures taken during its implementation. Finally in Chapter 5 we can find a conclusion to this thesis.

Chapter 2

Cryptography

2.1 Cryptography

Encryption is a method of transforming original data that are called plaintext or cleartext, into a form that appears to be random and unreadable and it is called ciphertext. Plaintext is either in a form that can be understood by a person (for example a document) or by a computer (like an executable code). Once the original data are transformed into ciphertext, neither human nor machine can properly process them until they are decrypted. This enables the transmission of confidential information over insecure channels without any unauthorized disclosure. When data is stored on a computer, it is usually protected by logical and physical access controls. When this same sensitive information is sent over a network, it can no longer take these controls for granted, and the information is in a much more vulnerable state.

Figure 2.1: The process of encryption and decryption.

A system that provides encryption and decryption is referred to as a *cryptosystem* and can be created through hardware components or program code in an application.

The cryptosystem uses an encryption algorithm, which determines how simple or complex the process will be. Most algorithms are complex mathematical formulas that are applied in a specific sequence to the plaintext. Most encryption methods use a secret value called a key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text, as depicted in Figure 2.2.

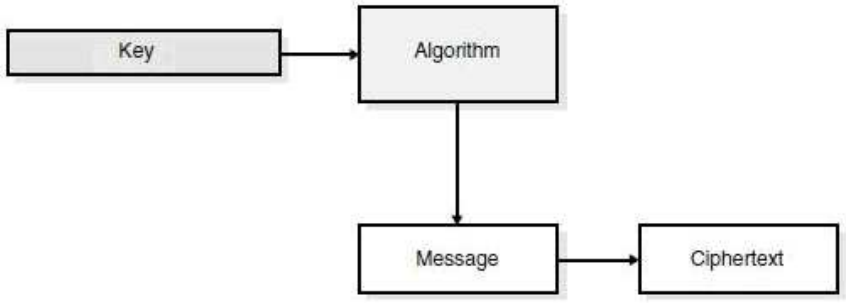

Figure 2.2: The role of the key in the encryption process.

The key is inserted into the mathematical algorithm and the result is applied to the message, which ends up in ciphertext.

The *algorithm*, the set of mathematical rules, dictates how enciphering and deciphering take place. Many algorithms are publicly known and are not the secret part of the encryption process. The way that encryption algorithms work can be kept secret from the public, but many of them are publicly known and well understood. If the internal mechanisms of the algorithm are not a secret, then something must be. The secret piece of using a well-known encryption algorithm is the key. The *key* can be any value that is made up of a large sequence of random bits. Is it just any random number of bits crammed together? Not really. An algorithm contains a *keyspace*, which is a range of values that can be used to construct a key. The key is made up of random values within the keyspace range. The larger the keyspace, the more available values can be used to represent different keys, and the more random the keys are, the harder it is for intruders to figure them out.

A large keyspace allows for more possible keys. The encryption algorithm should use the entire keyspace and choose the values to make up the keys as random as

possible. If a smaller keyspace were used, there would be fewer values to choose from when forming a key. This would increase an attacker's chance of figuring out the key value and deciphering the protected information.

2.2 Goals of Cryptosystems

Cryptosystems can provide confidentiality, authenticity, integrity, and non-repudiation services. It does not provide availability of data or systems. *Confidentiality* means that unauthorised parties cannot access information. *Authenticity* refers to validating the source of the message to ensure the sender is properly identified. *Integrity* provides assurance that the message was not modified during transmission, accidentally or intentionally. *Non-repudiation* means that a sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it. So if your boss sends you a message telling you that you will be receiving a raise that doubles your salary and it is encrypted, encryption methods can ensure that it really came from your boss, that someone did not alter it before it arrived to your computer, that no one else was able to read this message as it travelled over the network, and that your boss cannot deny sending the message later when he comes to his senses.

Different types of messages and transactions require a higher degree of one or all of the services that encryption methods can supply. Military and intelligence agencies are very concerned about keeping information confidential, so they would choose encryption mechanisms that provide a high degree of secrecy. Financial institutions care about confidentiality, but care more about the integrity of the data being transmitted, so the encryption mechanism they would choose may differ from the military's encryption methods. If messages were accepted that had a misplaced decimal point or zero, the ramifications could be far reaching in the financial institution world. Legal agencies may care more about the authenticity of messages that they receive. If information that was received ever needed to be presented in a court of law, its authenticity would certainly be questioned; therefore, the encryption method used should ensure

authenticity, which confirms who sent the information (Harris 2008).

2.3 Methods of Encryption

Cryptography algorithms use either secret or public keys. As if encryption was not complicated enough, the titles that are used to describe the key types only make it worse. Just pay close attention and we will get through this just fine.

2.3.1 Symmetric Cryptography

In a cryptosystem that uses symmetric cryptography, both parties will be using the same key for encryption and decryption. This provides dual functionality. As we said, symmetric keys are also called secret keys because this type of encryption relies on each user to keep the key a secret and properly protected. If this key got into an intruder's hand, that intruder would have the ability to decrypt any intercepted message encrypted with this key. Because both users use the same key to encrypt and decrypt messages, symmetric cryptosystems can provide confidentiality, but they cannot provide authentication or non-repudiation. There is no way to prove who actually sent a message if two people are using the exact same key. Symmetric cryptosystems have many problems and flaws like:

- Scalability – Each pair of users needs a unique pair of keys, so the number of keys grows exponentially.
- Key distribution – It requires a secure mechanism to deliver keys properly.
- Limited security – It can provide confidentiality, but not authenticity or non-repudiation.

Even with so many flaws symmetric cryptosystems are widely used because they are very fast and can be hard to break. Compared to asymmetric systems, symmetric algorithms scream in speed. They can encrypt and decrypt large amounts of data

that would take an unacceptable amount of time if an asymmetric algorithm was used instead. It is also very difficult to uncover data that is encrypted with a symmetric algorithm if a large key size was used.

There are two main types of symmetric algorithms: stream and block ciphers.

2.3.1.1 Block Ciphers

When a *block cipher* algorithm is used for encryption and decryption purposes, the message is divided into blocks of bits. These blocks are then put through substitution, transposition, and other mathematical functions. The algorithm dictates all the possible functions available to be used on the message, and it is the key that will determine what order these functions will take place. Strong algorithms make reengineering, or trying to figure out all the functions that took place on the message, basically impossible.

The properties of a cipher should contain confusion and diffusion. Different unknown key values cause confusion, because the attacker does not know these values, and diffusion is accomplished by putting the bits within the plaintext through many different functions so that they are dispersed throughout the algorithm. Block ciphers use diffusion and confusion in their methods. A simple block cipher has 16 inputs and each input represents a bit. This block cipher has two layers of 4-bit substitution boxes called S-boxes. Each S-box contains a lookup table that instructs how the bits should be permuted or moved around. The key that is used in the encryption process dictates what S-boxes are used and in what order.

The key dictates what S-boxes are to be used when scrambling the original message from readable plaintext to encrypted non-readable ciphertext. Each S-box can have different types of functions, mathematical formulas, and methods to be performed on each particular bit. The key provides the confusion because the attacker would not know which S-boxes would be used during the encryption process and all the permutations that happen on the bits is the diffusion, because they are moved between

different S-boxes and put through different steps of scrambling.

Most block ciphers work with blocks of 64 bits and many more S-boxes are usually involved. Strong and efficient block cryptosystems use random key values so an attacker cannot find a pattern as to which S-boxes are chosen and used.

2.3.1.2 Stream Cipher

While a *block cipher* performs mathematical functions on blocks of data, a stream cipher does not divide a message up into blocks but treats the message as a stream of bits or bytes and performs mathematical functions on them individually.

When using a stream cipher, the same plaintext bit or byte will be transformed into a different ciphertext bit or byte each time it is encrypted. Some stream ciphers use a *key-stream generator*, which produces a stream of bits that is XORed with the plaintext bits to produce ciphertext (XOR stands for exclusive OR).

If the cryptosystem was only dependent upon this key-stream generator, an attacker could get a copy of the plaintext and the resulting ciphertext, XOR them together, and find the key-stream to use in decrypting other messages. So the smart people decided to stick a key into the mix.

In block ciphers, it is the key that determines what functions are applied to the plaintext and in what order. It is the key that provides the randomness of the encryption process. Because most encryption algorithms are public, people know how they work. So the secret to the secret sauce is the key. In stream ciphers, the key also provides randomness, but to the key-stream that is actually applied to the plaintext. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the key-stream data.

A strong and effective stream cipher algorithm contains the following characteristics:

- Long periods of no repeating patterns within key-stream values.
- Statistically unpredictable.
- The key-stream is not linearly related to the key.

- Statistically unbiased key-stream (as many 0's as 1's).

Because stream ciphers encrypt and decrypt one bit at a time, they are more suitable for hardware implementations. Block ciphers are easier to implement in software because they work with blocks of data that the software is used to working with, which is usually the width of a data bus (64 bits). Stream ciphers are intensive because each bit must be manipulated, which works better at the silicon level. To make things just a little more confusing, block ciphers sometimes work in a mode that emulates a stream cipher.

Different steps and algorithms provide different types of security services:

- A message can be encrypted, which provides confidentiality.
- A message can be hashed, which provides integrity
- A message can be digitally signed, which provides authentication and integrity.
- A message can be encrypted and digitally signed, which provides confidentiality, authentication, and integrity (Harris 2008).

Some examples of symmetric key cryptography algorithms are:

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Blowfish
- IDEA
- RC4, RC5, and RC6

2.3.2 Asymmetric Cryptography

In symmetric key cryptography, a single secret key is used between entities, whereas in public key systems, each entity has different keys, or *asymmetric keys*. The two

different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required to decrypt the message.

In a public key system, the pair of keys is made up of one public key and one private key. The *public key* can be known to everyone, and the *private key* must only be known to the owner. Many times, public keys are listed in directories and databases of e-mail addresses so they are available to anyone who wants to use these keys to encrypt or decrypt data when communicating with a particular person. The public and private keys are mathematically related, but cannot be derived from each other.

If confidentiality is the most important security service to a sender, the file will be encrypted with the receiver's public key. This is called a *secure message format* because it can only be decrypted by the person who has the corresponding private key. If authentication is the most important security service to the sender, then asymmetric cryptography would encrypt the message with her private key. This provides assurance to the receiver that the only person who could have encrypted the message is the individual who has possession of that private key. If the sender encrypted the message with the receiver's public key, authentication is not provided because this public key is available to anyone.

Encrypting a message with the sender's private key is called an *open message format* because anyone with a copy of the corresponding public key can decrypt the message; thus, confidentiality is not ensured.

Some examples of asymmetric key cryptography algorithms are:

- RSA
- Elliptic Curve Cryptosystem (ECC)
- Diffie–Hellman
- El Gamal
- Digital Signature Standard (DSS)

(Harris 2008)

2.4 DES

DES is a block encryption algorithm in which when 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out. It is also a symmetric algorithm, meaning the same key is used for encryption and decryption. It uses a 64-bit key, 56 bits make up the true key, and 8 bits are used for parity.

2.4.1 DES Modes of Operation

DES has four distinct modes of operation that are used in different situations for different types of results.

2.4.1.1 Electronic Code Book (ECB) Mode

This mode is the native encryption method for DES and operates like a code book. A 64-bit data block is entered into the algorithm with a key and a block of ciphertext is produced. For a given block of plaintext and a given key, the same block of ciphertext is always produced.

Every key has a different code book which provides the recipe of substitutions and permutations that will be performed on the block of plaintext. Because this mode works with blocks of data independently, data within a file does not have to be encrypted in a certain order. This is very helpful when using encryption in databases. A database has different pieces of data accessed in a random fashion. If it is encrypted in ECB mode, then any record or table can be added, encrypted, deleted, or decrypted independent of any other table or record.

This mode is usually used for small amounts of data like encrypting and protecting encryption keys. It is used for challenge-response operations and some key management tasks. It is also used to encrypt personal identification numbers (PINs) in ATM machines for financial institutions and it is not used to encrypt large amounts of data because patterns would eventually show themselves.

2.4.1.2 Cipher Block Chaining (CBC) Mode

In ECB mode, a block of plaintext and a key will always give the same ciphertext. This can show evidence of a pattern, which if an evildoer put some effort into revealing, could get him a step closer to compromising the encryption process. CBC does not reveal a pattern because each block of text, the key, and the value based on the previous block is processed in the algorithm and applied to the next block of text. This gives a more random resulting ciphertext. A value is extracted and used from the previous block of text. This provides dependence between the blocks and in a sense they are chained together. This is where the title of Cipher Block Chaining (CBC) comes from, and it is this chaining effect that hides any repeated patterns. The results of one block are fed into the next block, meaning that each block is used to modify the following block. This chaining effect means that a particular ciphertext block is dependent upon all blocks before it, not just the previous block.

2.4.1.3 Cipher Feedback (CFB) Mode

In this mode, the previously generated ciphertext from the last encrypted block of data is inputted into the algorithm to generate random values. These random values are processed with the current block of plaintext to create ciphertext. This is another way of chaining blocks of text together, but instead of using a value from the last data block, CFB mode uses the previous data block in the ciphertext and runs it through a function and combines it with the next block in line. This mode is used when encrypting individual characters is required.

2.4.1.4 Output Feedback (OFB) Mode

This mode is very similar to Cipher Feedback (CFB) mode, but if DES is working in Output Feedback (OFB) mode, it is functioning like a stream cipher by generating a stream of random binary bits to be combined with the plaintext to create ciphertext. The ciphertext is fed back to the algorithm to form a portion of the next input to

encrypt the next stream of bits. In OFB mode, the DES block cipher crosses the line between block cipher and stream cipher and uses a keystream for encryption and decryption purposes.

(Harris 2008)

2.4.2 Triple DES (3DES)

In the development of my thesis the encryption that was used in order to secure the communication between the sensor and the server is the triple des.

Triple-DES is an extension of Data Encryption Standard (DES) that results in a more complex but more secure block cipher. Standard DES represents a component in Triple-DES architecture. If $E_K(I)$ and $D_K(I)$ denote the DES encryption and decryption of I using DES key K, respectively, then Triple-DES encryption and decryption is performed as follows:

$$\text{Encryption} : E_{K_3}(D_{K_2}(E_{K_1}(I))) = O$$

$$\text{Decryption} : D_{K_1}(E_{K_2}(D_{K_3}(O))) = I$$

2.4.3 Triple-DES Encryption/Decryption Process

The encryption/decryption process is equivalent to performing three standard DES encryption/decryption sequences. The Standard Triple-DES core iteratively performs the DES encryption/decryption process. Fast Triple-DES implementation contains three DES modules arranged in a pipelined architecture. Thus, the first output block is obtained in three times the time needed by a single DES core. However, each subsequent input block can be fed to the core in the time needed for a single DES encryption/decryption. If the input feed to the core is maintained constant in this respect, each output block, save the first, is obtained after time needed to perform single DES processing (Systems 2006).

Triple DES takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (rightmost) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process (VOCAL Technologies 2004).

2.5 Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard) is a symmetric-key encryption standard adopted by the U.S. government and is the current encryption standard. The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Other input, output and Cipher Key lengths are not permitted by this standard.

The AES cipher is specified as a number of repetitions of transformation rounds

	AES	Triple-DES
Description	Advanced Encryption Standard	Triple Data Encryption Standard
Timeline	Standard since 2001	Standard since 1977
Type of algorithm	Symmetric	Symmetric
Key size (bits)	192	168
Speed	High	Low
Time to crack (with 255 tries per sec)	149 trillion years	4.6 billion years
Resource consumption	Low	Medium

Table 2.1: AES vs Triple-DES.

that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key (Chouinard 2002).

2.6 Cryptographic Hash Functions

Hash functions are functions that compress an input of arbitrary length to a result with a fixed length. If hash functions satisfy additional requirements, they are a very powerful tool in the design of techniques to protect the authenticity of information. Hash functions are used to allocate as uniformly as possible storage for the records of a file.

2.6.1 One-way hash function (OWHF)

An one-way hash function is a function h satisfying the following conditions:

- The description of h must be publicly known and should not require any secret information for its.
- The argument X can be of arbitrary length and the result $h(X)$ has a fixed length of n bits (with $n \geq 64$).

- Given h and X, the computation of $h(X)$ must be "easy".
- The hash function must be one-way in the sense that given a Y in the image of h, it is "hard" to find a message X such that $h(X) = Y$ and given X and $h(X)$ it is "hard" to find a message $X' \neq X$ such that $h(X_0) = h(X)$.

The first part of the last condition corresponds to the intuitive concept of one-wayness, namely that it is "hard" to find a preimage of a given value in the range. In the case of permutations or injective functions only this concept is relevant. The second part of this condition, namely that finding a second preimage should be hard, is a stronger condition that is relevant for most applications.

2.6.2 Collision resistant hash function (CRHF)

A collision resistant hash function is a function h satisfying the following conditions:

- The description of h must be publicly known and should not require any secret information for its operation (extension of Kerckhoffs's principle).
- The argument X can be of arbitrary length and the result $h(X)$ has a fixed length of n bits (with $n \geq 128$).
- Given h and X, the computation of $h(X)$ must be "easy".
- The hash function must be one-way in the sense that given a Y in the image of h, it is "hard" to find a message X such that $h(X) = Y$ and given X and $h(X)$ it is "hard" to find a message $X' \neq X$ such that $h(X') = h(X)$.
- The hash function must be collision resistant: this means that it is "hard" to find two distinct messages that hash to the same result (PRENEEL 2003).

2.7 Digital Signatures

A digital signature is an encrypted hash value. If for example a person A wanted to ensure that the message he sent to a person B was not modified and he wants the other person to be sure that it came only from him, he can digitally sign the message. This means that a one-way hashing function would be run on the message and then person A would encrypt that hash value with his private key.

When person B receives the message, he will perform the hashing function on the message and come up with his own hash value. Then he will decrypt the sent hash value with the sender's public key. Then he compares the two values and if they are the same, he can be sure that the message was not altered during transmission and that the message came from person A because the value was encrypted with his private key.

The hashing function ensures the integrity of the message and the signing of the hash value provides authentication and non-repudiation. The act of signing just means that the value was encrypted with a private key.

2.7.1 The Digital Signature Standard (DSS)

Because digital signatures can hold such importance on proving who sent what messages and when, the government decided to erect standards pertaining to its functions and acceptable use. In 1991, NIST proposed a federal standard called the Digital Signature Standard (DSS). It was developed for federal departments and agencies, but most vendors designed their products to meet these specifications also. The federal government requires its departments to use the Digital Signature Algorithm (DSA) and the Secure Hash Algorithm (SHA). The SHA creates a 160-bit output, which is then input into the DSA. The SHA is used to ensure the integrity of the message and the DSA is used to digitally sign the message. This is an example of how two different algorithms are combined to provide the right combination of security services.

RSA and DSA are the best known and most widely used digital signature algo-

rithms. Unlike RSA, DSA can only be used for digital signatures and is part of the DSS. RSA can be used for digital signatures and message encryption (Harris 2008).

Chapter 3

Biometric Sensors

3.1 Biometric Identification Process

Many systems use biometric characteristics to authenticate users. A biometric is a physical or biological feature or attribute that can be measured. The biometric is something that is part of you, rather than something you know or can carry with you.

Examples of physiological biometric features include: height, weight, the shape of the hand (palm geometry), the voice, the pattern of veins, retina or iris, the face and fingerprints. Examples of behavioural biometrics are voice patterns, signature and keystroke sequences and even the body movement while walking.

Biometric identification works in four stages:

- **Enrolment**: where a record associating the identifying features with the individual is created.
- **Storage**: where a record of that scan is stored either in a central database, or it can be stored in a decentralised way.
- **Acquisition**: during identification a new biometric sample is gathered.
- **Matching**: when the new biometric sample is compared to the stored. If these two match, the identification is successful.

Biometric identification is a statistical process. Variations in conditions between enrolment and acquisition as well as bodily changes (temporary or permanent) mean that there is never an exact match like when a password or a PIN is given and therefore there is no clear line between a match and a non-match. So an existing match depends not only on the two data sets to be compared, but also on what margin of error is deemed tolerable (European Commission JRC 2005).

3.1.1 Acquisition of Biometric Samples

Acquisition is the first contact of the user with the biometric system. The user's biometric sample is obtained using an input device (sensor). The quality of the first biometric sample is very important because this sample will be used for future authentications.

Acquisition is the first contact of the user with the biometric system. The user's biometric sample is obtained using an input device (sensor). The quality of the first biometric sample is very important because this sample will be used for future authentications.

Commonly used biometric traits include fingerprint, face, iris, hand geometry, voice, palm-print, handwritten signatures and gait. Biometric systems usually extract a salient set of features which are widely known as templates from the biometric data of a user. A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample. The template is a compact description of the biometric sample and it can not reveal by its own crucial information about the original data. Templates can vary between biometric modalities as well as vendors. All biometric devices are not based on templates (for example voice recognition based on "models").

3.1.2 Storage of Biometric Templates

The biometric measurements are processed after the acquisition and some features are extracted. After processing the biometric samples, the newly obtained master template

has to be stored. The template can be stored:

- in a card
- in the central database on a server
- on a workstation
- in an authentication terminal

After the enrolment and for successful authentications or identifications a fully automated process does the following:

Biometric measurements must be stored so that the system can make comparison with the master template. Often sensors check if the measurements obtained really belong to a live person. The biometric measurements obtained are processed in order new characteristics to be computed.

3.1.3 Matching/Authentication Process

These new characteristics are compared with the characteristics obtained during enrolment. If the system performs can verify them then they are compared only to the master template. For an identification request the new characteristics are compared with a large number of master templates.

The final verification process is the "yes or no" decision which is based on a threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value (Matyas & Riha 2002).

3.2 Success Factors for Biometrics

When an organisation or a company wants implement a biometric identification system there are eight critical success factors that should be considered:

- **Accuracy**: Biometric devices are improving more and more as the years are passing but even today there are still no guarantees of a device having 100 percent

accuracy. It's up to organisations to select the level of inaccuracy they and their employees can tolerate. When judging error rates, two types of errors should be considered:

- The first type of errors includes all instances in which a biometric system denies access to an authorised user.
- The identification of an unauthorised user as an authorised user is an example of a second type error.

By adjusting the sensitivity of the biometric sensor the occurrence of each error type can be increased or decreased but decreasing one type of errors, will increase the other type of errors. The main objective when implementing a biometric system is the proper balance between these two error types. The most common method is to focus on the Cross-over Error Rate (CER). This is the point at which the frequency of the first type of errors (False Rejection Rate or FRR) and the frequency of the second type of errors (False Acceptance Rate or FRR) are equal. The CER is the best indicator of overall accuracy and it is expressed as a percentage with lower values being better.

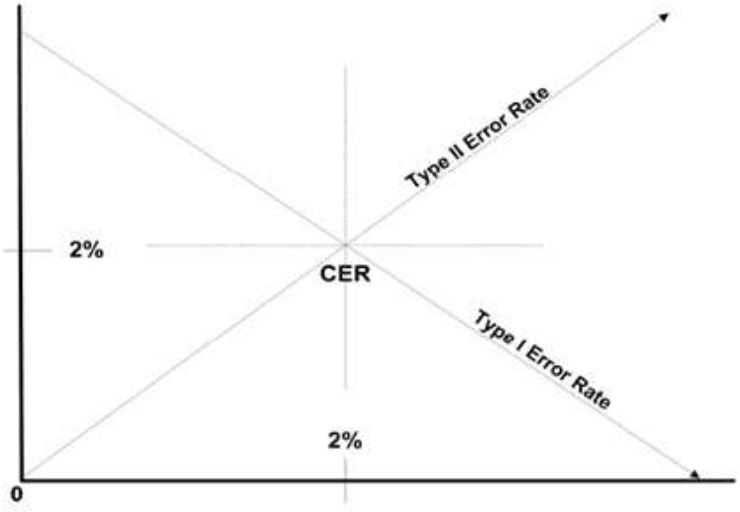

Figure 3.1: CER and Error Rate Relationship.

- **Speed**: The most important factor in use of biometrics is the speed at which

a sensor and its controlling software accepts or rejects authentication attempts. The effective throughput, or how many users a biometric sensor can process in a given period, is a function of the entire authentication process.

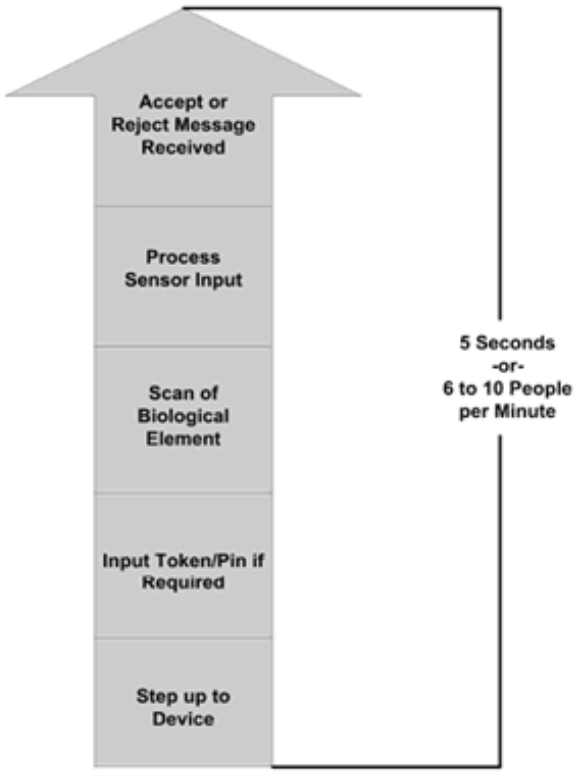

Figure 3.2: Biometric Authentication Process.

InFigure 3.2 the various stages involved through authentication are shown. Acceptable throughput is typically five seconds per person or six to ten people per minute. User frustration begins to set in at lower throughput rates.

- **Resistance to counterfeiting**: Some biometric sensors are more susceptible to counterfeiting from others. For example, some early systems allowed an intruder to use lifted finger or hand prints to gain entry and so it was much easier for an attacker to gain authentication. Today's systems are, in general, more sophisticated as they use the entire geometry of a finger or hand instead of just the line patterns that make up prints.

- **Reliability**: Sensors must continue to operate at a low CER between failures. A

gradual degradation in throughput affects user acceptability and organisational productivity.

- **Data storage requirements**: The amount of storage space that is necessary in order to support a biometric system depends on what data is actually stored. Voice recognition systems for example might use a great deal of storage space as voice files are usually large. On the other hand finger architecture recognition technology, simply stores a relatively small hash value created when a user is enrolled and so the storage space required is much less from voice recognition systems. Whenever a sensor scans the finger again, it re-computes the hash value and compares it to the stored value. At all biometric systems the impact on the storage environment is very important.

- **Enrollment time**: One more factor that could influence a user's acceptance is the time required to enroll a new user into the biometric system. An acceptable enrollment duration is usually two minutes or less per person. This enrollment rate not only reduces employee frustration but it also helps reduce administrative costs associated with system management.

- **Perceived intrusiveness**: Second only to throughput, the amount of personal intrusiveness a sensor presents to organisations employees is a key determinant when assessing user acceptance. Some common fears that grow out of biometric implementations are:

  - Fear that the company stores unique personal information.
  - Fear that the company is collecting personal health information (retinal scans look at patterns that are also used to determine certain health conditions) for insurance purposes.
  - Fear that the red light in retinal scanning sensors is physically harmful.
  - Fear of contracting diseases through contact with publicly used sensors.

- **User acceptance**: User acceptance does not depend on how a company perceive biometric authentication but it depends on how the company's employees perceive it (Olzak 2006).

3.3 Verification, Identification, Screening

3.3.1 Verification

Verification is a 1-to-1 matching test in order to ensure whether person is really who he claims to be. There are two verification types:

3.3.1.1 Verification with centralised storage

If a centralised database (produced at enrolment and updated with every additional user after) which contains all biometric data and the associated identities exists, then the verification process is done by comparing the live with the stored sample. There are two possible error types at verification:

- a false match (a person is not who he claims to be but the system erroneously accepts him).
- a false reject (a person is who he claims to be but the system fails to make the match).

It's easy to understand that false matches are more insidious than false rejects as they may allow a fraudulent individual to pass with the mistake going unnoticed by the system while false rejects can only cause unnecessary inconvenience.

3.3.1.2 Verification with distributed storage

This is the case where biometric data are stored in a memory device carried by the person (like a smart card or a chip integrated into an identity document) and the person will provide a live biometric sample which will be compared to the biometric

data stored on the memory device. This can be achieved by the verification system which retrieves the person's biometric data from the memory device and compares them to the live sample, or by the memory device itself. The identity details can be stored on the memory device or they can be written on the accompanying documents (for example in the case of a passport, identity information might be printed next to the chip). If verification is successful, then the person is confirmed to be who he claims. Like the previous case, false acceptance and false rejection errors can also occur. Moreover, there is the possibility that the documentation or the memory device are fraudulent or have been tampered with.

3.3.2 Identification

Identification is a 1-to-many matching test in order to find out the identity of an individual when it is unknown, in other words when the user makes no claim of identity. Unlike verification, here a central database is needed which keeps records for all people known to the system. Without a database of records, the process of identification is not possible.

When a user wants to be identified, he provides a live biometric sample which is processed and the resulting biometric template is compared against all the entries in the database to find a match (or a list of possible matches). The system then returns as a response the match (or list of possible matches) existing, or that there is no match found against the enrolled population. During identification false match or false reject errors are possible to occur. Maintenance of the integrity of databases used in identification processes is essential in protecting individuals from identity theft.

3.3.3 Screening

Screening is a processing type which uses a database or watch-list. A watch-list contains data of people who are apprehended or excluded. Records on the watch-list may contain only biometric data for someone who is wanted or it may contain identity

information, depending on what is known. Everyone passing the screening process provides a biometric sample, in order to be checked for possible matches against the watch-list. The key feature of a watch-list is that people will only be identified if they appear on the list. If no match occurs the person pass through without having his biometrical sample stored in a database. Screening is very useful at border control or covertly, such as scanning a crowd with the use of security cameras (European Commission JRC 2005).

3.4 Advantages and Disadvantages of biometric authentication systems

3.4.1 Advantages

The key advantage of biometric authentication methods over other user authentication methods is that they actually authenticate the user by using real human physiological or behavioural. Biometric characteristics are permanent and not changeable and it is really hard to change one's fingerprint, iris or other biometric characteristics. Moreover users cannot pass their biometric characteristics to other users like they can with cards or passwords. Also biometrics cannot be stolen. Biometric characteristics are not secret and therefore the availability of a user's fingerprint or iris pattern does not break security the same way as availability of the user's password. Even the use of dead or artificial biometric characteristics should not let the attacker in.

Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be avoided, thus saving some costs of the system management.

Another advantage of biometric authentication systems may be their speed because a user can be authenticated much quicker using an iris-based identification system rather than finding a key ring, locating the right key or typing a password.

3.4.2 Disadvantages

Biometric authentication methods have also some disadvantages. Biometric systems still need improvement because their performance is not ideal. Although few biometric systems are fast and accurate enough to allow identification, most of current systems are suitable for the verification only, as the false acceptance rate is too high.

Another disadvantage is that not all users can use any given biometric system (e.g. people without hands are not able to use fingerprint or hand-based systems and also visually impaired people have difficulties using iris or retina based techniques).

Biometric data are not secret and for that reason systems can authenticate a user only just after receiving the correct biometric characteristics and only when user's characteristics are fresh and have been collected from the user being authenticated. This means that the biometric input device must be trusted. The input device also should be under human supervision or tamper-resistant. The fact that biometric characteristics are not secret brings some issues that common authentication systems need not deal with. Many of the current biometric systems are not aware of this fact and therefore the security level they offer is limited.

One more drawback that biometric authentication methods might have is that some biometric sensors have a limited lifetime while a magnetic card reader for example can be used for many years, the optical fingerprint reader for example must be regularly cleaned and even then the lifetime need not exceed one year.

Another disadvantage those systems have is that they may violate user's privacy as biometric characteristics are sensitive data that may contain a lot of personal information. The DNA for example contains the user's preposition to diseases.

Also use of biometric systems also implies loss of anonymity. Unlike others systems where users can have multiple identities when authentication methods are based on something the user knows or has, biometric systems can sometimes link all user actions to a single identity. Finally one more problem is that some users find some biometric systems intrusive or personally invasive. Even if biometric systems are not dangerous

at all, users are occasionally afraid of something they do not know much about. In some countries people do not like to touch something that has already been touched many times, while in other countries people do not like to be photographed or their faces are completely covered (Matyas & Riha 2002).

3.5 The Security Problem in Biometric Systems

Security is a major issue when it involves sensor networks with biometric-based authentication systems. Security problems are even more important nowadays, as most of the real-world implementations usually include remote data capturing, wired or wireless communications, sensor devices, distributed data management and other related technologies and systems. In order to build a secure biometric system, every component needs to be able to communicate securely because without this 'weak links' will appear, which probably will be targeted by potential attackers. One key problem that biometric information systems have is where to store the biometric templates (the biometric samples that will be used for comparison to the submitted samples). The following three options have been identified as the most typical ones:

- Store the template in the biometric reader itself.
- Store the template in a remote central repository.
- Store the template on a portable token, such as a smart card.

Most biometric-based systems need to have a distributed configuration for practical use and for that reason biometric templates are usually stored in a location remote to the sensor. The biometric information sensor is therefore faced up with the following issues:

- Acquisition of the authentic biometric reading.
- Secure/authenticated transmission of the biometric data to the processing centre.

- Secure/authenticated transmission of the result from the comparison of the two samples, from the processing centre.

Now in the case where the template is stored on a portable token the biometric sensor can only verify whether it matches the biometric characteristics of its holder, or not and it can't associate the template with the true identity of its holder.

The most important step for a secure biometric information system is to authenticate a biometric sensor to the system. In order to accomplish this, a unique ID can be stored in a smart card that is inserted into the biometric sensor. The latter will send a reading to the processing centre if and only if the ID proves to be a legitimate one. The drawback in this case is that the smart card can be physically attacked with an electronic device and the unique ID could be stolen. If this ID gets attacked the original smart card could then be duplicated and then all applicable attacks against the sensor can be launched. The use of cryptographic techniques can help in providing solutions to the problem of sensor authentication (Papanikolaou, Ilioudis, Georgiadis & Pimenidis 2008).

3.5.1 Attacks on Biometric Systems

Even though biometric systems have many advantages they are also vulnerable to many types of attacks, which can affect their security. The attacks can be classified into several categories.

Denial of Service (DoS) attacks are usual attacks in the biometric sensors and can be physical damage (like using strobe lights against optical sensors or liquid on sensors etc.) or power loss to the system attacks designed degrade the performance of sensors and the quality of data.

Presenting a fake biometric to the sensor is one attack that may take place in biometric sensors. With a fake biometric, the enrolment data will be an accurate but the real identity will be incorrect and as a result the system will grant to the wrong user access privileges. These attacks are conducted at the entry point of a system and

digital protection mechanisms, like encryption and digital signatures, are not effective. Many biometrics (including fingerprints, hand and iris) are subject to this form of attack and also submitting a previously intercepted biometric is effectively a replay attack (Roberts 2006).

Also a possible attack may occur on the template database which can add a new template, modify or remove existing templates and others. Database is an easier target as templates are smaller and the data sets less complex than the unprocessed biometric data. Moreover the transmission medium between the template database and matcher can be attacked and result in the alteration of the transmitted templates. Matcher can be modified to output an artificially high matching score.

Additionally with other attacks the feature extractor module can be compromised to produce feature values selected by the attacker. In other cases genuine feature values are replaced with the ones selected by the attacker. Finally, in another type of attack, the matcher result (accept or reject) can be overridden by the attacker (Uludag & Jain 2004).

3.5.2 Errors on Biometric Systems

As Elliott & Kukula (2009) have stated, several errors may occur in a biometric system by the interaction of humans with biometric devices and they also described six new definitions. In this thesis, it will be assumed that the extraction of the user's biometric sample by the sensor is an error-free process.

3.6 Social, Economic, Legal and Technical Issues

Security and privacy are the obvious challenges when studying the deployment of biometrics but there are also some social, economic, legal and technical (SELT) implications of biometrics for society. From their contributions, the following subjects emerge as the key characteristics of the transition to the biometric society.

3.6.1 Social

The spread of biometrics and as a result the replacement of any weak or no identification systems at all by strong ones may reduce the scope for privacy and anonymity of citizens. As a result this may challenge the existing trust model between citizen and state and if governments become more efficient at identifying citizens in all kinds of situations with biometric authentication systems, that trust model is very likely to change.

It is easy for everyone to understand that, it is important to be clear on the purposes of introducing biometrics and realistic about their performance.

- Concerning the former, it has to be considered the possibility that "function creep" will set in over time. This means that biometrics will be used for purposes other than those meant and agreed at the time of introduction and enrollment. For example, several separate biometric databases could be connected in the future.

- Concerning the latter, if biometrics by somehow stop having any kind of threat to society, expectations are bound to be disappointed and citizens might come to feel "cheated". In that case, the automated decision-making may be resented even more than it would otherwise.

One more important point is that, biometrics are not able to work alone but need a fallback procedure. For several reasons, like disabilities, age or sickness, a significant number of people might not be able to participate in an automated biometric identity verification process. Similar procedures need to be foreseen for these people and if someone's fingerprint for example is not easily legible, that should not make him a second-class citizen.

3.6.2 Economic

Authentication systems based on biometrics provide strong identification but from the economic point of view this is not always the optimal solution, as identification imposes a cost, which will only be compensated by the benefits of identity if these benefits are large enough. Also, an assessment of costs of biometrics should look at the cost of technologies and should encompass the complete identification process, including for example, the costs of backup procedures.

Moreover, a secure and effective identification lowers the risk of possible attackers to penetrate the system and as a result any additional inside measures will be less efficient, thus leading to their disappearance, which means that once the outer wall is breached, the intruder will then have full access. As a result, an identity theft may simultaneously become less likely and much more serious.

Regarding the market development, the biometrics market has many characteristics which make a competitive market equilibrium unlikely. It is a network industry with strong complementary, a tendency to "tipping", a few large launch projects establishing considerable first-mover advantage, and ample scope to use intellectual property rights to reduce or even prevent competition. For that reason governments should ensure that the market will develop into a competitive one just like open source software.

3.6.3 Legal

The current existing legal environment in Europe is flexible and does not inhibit the introduction of biometrics yet, it has very few specific provisions regarding the impact of biometrics on privacy and data protection. Existing legal environment about data protection does influence the implementation of biometrics, but it does not contain normative content and so some interpretation problems still exist and so consequently, new legislation will be needed when new applications become compulsory or when biometrics become widely used.

Such legislation should be based on two pillars:

- opacity
- transparency

On the one hand, opacity rules (privacy rules) should prevent inappropriate collection of biometric data and they should inform the users properly about the conditions under which the use of biometrics will be allowed but also on the other hand, if use is allowed, transparency rules (data protection rules) should indicate how the data can be processed and how the processing can be traced. Nowadays users don't usually consider the repercussions of an enrolment process, even if strong identity is not required in most cases. An evaluation of whether a biometric application is appropriate and how it will operate should always consider local storage, proportionality, whether a less intrusive method exists, reliability and consent and of course data encryption should be mandatory.

3.6.4 Technical

Biometric characteristics are different from paper documents or secret codes. These characteristics cannot be lost or stolen and also they cannot be revoked. Many of those characteristics like face or voice are in the public domain as everyone can see them. A biometric match is never 100 percent certain because the match depends as much on the threshold of acceptance as it does on the two sets of data to be compared. Users making verifications and those being verified need to know the variability of the threshold and how that may change depending on the application. They should also know that the biometric technology itself is nothing more but a part of the whole security system, which will work well only if the acquisition environment is properly set up, if the storage is secure and also if the enrolment process is sufficiently controlled (European Commission JRC 2005).

3.7 Medical Aspects of Biometrics

Biometrics, just like many other new technologies in the past, cause public concerns about possible damage to the human body derived from the use of physiological data. For that reason, the perception of any potential implications on health and risks associated with the use of biometric devices, including also fears about the secondary uses of data acquired should not be underestimated. There are two types of medical implications:

- direct medical implications (DMI)
- indirect medical implications (IMI)

The first one is about the potential risks of damage associated with the use of biometric devices, and the other one is related to the ethical risk of revealing private medical information. Both types of medical implications are like fuzzy quantifications of risks, but DMI refer to physical, measurable potential damaging effects, while IMI are about the possibility of extracting medical information that could be used not only for identification and verification but for other purposes too.

3.7.1 Direct Medical Implications

There are not many cases that may cause direct medical implications (DMI). One method that includes potential DMI is retinal scanning, which analyses the layer of blood vessels at the back of the eye. In this method the scanner uses infrared radiation and which is possible to cause thermal injury on the back of the eye. Exaggerative heating could also cause harm the cornea and the lens, even if there is not decent evidence on these effects when retinal scanning sensors are used. It is important to say that, despite the fact that these techniques are not widely spread in the market, many companies want to develop new systems based on retinal scanning. Other biometric techniques, like three dimensional (3D) face recognition using laser may also include potential DMI.

Iris recognition is one of the most widely used biometric technologies and the concerns related to these systems are the same as those for retinal scanning, namely that the eye might suffer thermal damage from prolonged exposure to infrared (IR) radiation. The truth although is that iris recognition systems, in order to cause actual damage would need much higher doses of radiation than imaging sensors usually use. It is easy for everybody to understand that by looking directly into the sun for some time the eyes are very possible to suffer damages but the energy that enters into the eye during an exposure to an IR sensor is far less than that received just by standing in sunlight or by looking at an incandescent lamp. The enrolment process during iris recognition can take from 30 seconds to 2 or 3 minutes but even during this time period, the radiation absorbed is very low and with no significant implications for the eye and that's why no evidence of medical risks have been reported despite the wide use of iris-based biometrics.

Biometrics that require physical contact with sensors, like systems based on fingerprints or hand geometry, are sometimes perceived as a source of potential germ transmission. People don't always want to use such kind of sensors because of the fear of contamination. However, this is more a perception problem rather than an actual health risk and of course there are other daily actions similar in nature, like touching doorknobs, railings or other common objects which also involve the risk of contamination. Hand geometry sensors could have more potential for cross -contamination than fingerprint sensors, but this does not cause widespread health concerns. General counter-measures for cross-contamination are irradiation with UV light at regular intervals or even the use of nanomaterials that prevent the spread of bacteria.

3.7.2 Indirect Medical Implications

Indirect Medical Implications (IMI) refers to fears about secondary use of health data, which may lead to important ethical considerations. As regards the potential barriers to biometrics implementation, IMI are, indeed, much more relevant than DMI. The ethical

issue becomes extremely important particularly when people's genetic information may be at stake. Even if genetic data, being acquired during the enrollment process, are not usable for second purposes the general perception is that individuals' DNA could be captured and, for that reason genetic predispositions and conditions could be revealed without their concurrence.

DNA is not currently being used for real-time identification and so these issues have not yet been a real problem. For currently used biometric systems, IMI are related to the detection of vascular malfunction, the interaction with 'iridology', and also the detection of emotional conditions.

The detection of any possible vascular malfunction has been mainly associated with retinal scanning. Although the pattern formed by the blood vessels in the retina is able to give information about vascular conditions, the known retinal scanning techniques are not able to provide direct information about the retina but despite that, some further monitoring and analysis should be done whenever a new biometric system that scans this tissue is put on the market.

'Iridology' which is the study of iris texture claims that important alterations in the iris pattern indicate the state of health of each of the organs a human's body, one's mood or even his personality. Iridology is considered questionable by scientists, who often consider it to be like palm-reading, and as a result it is not recognised as a medical procedure. Yet, because of its respective popularity in Europe, iridology could raise concerns for iris recognition methods which could have an impact on its widespread adoption. For this reason some additional issues are presented in order to disperse fears over indirect acquisition of data that iridologists claim to be possible. The first is that the image acquired during the enrollment process is black and white, which eliminates much of the basis for eliciting such information, secondly, in most cases only the image template is stored (which means that the full image isn't stored), and thirdly when the iris image appears on the screen, it is intentionally blurred.

Face recognition techniques also cause fears of revealing the emotional state of a

person but, the data acquired during this process are not meant to reveal such kind of information. Additionally, users are requested to exhibit strictly neutral expressions for the face recognition sample acquisition process in order to perform it properly.

3.7.3 IMI from DNA

IMI originated from DNA are a special source of public concern, and probably the most controversial case. The main issue of this controversy is obviously influencing the public acceptance of biometric systems that analyze DNA, since people fear the possible manipulation or misuse of their genetic data. The completion of the human genome sequence announced several years ago and the decision of some governments to store the DNA of citizens for pharmaceutical research, and the extended use for DNA profiling in forensics, are the main factors that raise strong privacy concerns. Some characteristics inherent to current DNA biometric practices, however, could reassure the general public about the failure of these techniques to perform genetic profiling of individuals. For example, only extracts of DNA that are not at present connected to any genetic information are actually stored and used to perform the matching process, while the physical individual's sample is not stored at all (European Commission JRC 2005).

3.8 Biometrics History

The term "biometrics" is based on two Greek words, the word "bio" (which means "life") and the word "metrics" (which means "to measure"). Automated biometric systems have only been available over the last few decades, as a result to the significant advances in the field of computer processing despite the fact that many of these new automated techniques are based on ideas that were originally conceived hundreds or even thousands of years ago.

One of the oldest characteristic used for recognition by humans is their face. Since the beginning of civilisation, humans have used only faces in order to identify known

and unknown persons. This simple procedure became more and more challenging through the decades as populations increased. The concept of human-to-human recognition is also seen in behavioural-predominant biometrics such as speaker and gait recognition. People use these characteristics, and in many cases even unconsciously, so as they can recognise known individuals on a daily basis.

Through the history of civilisation some other characteristics have also been used as a more formal way of recognition and some characteristic examples are:

- In a cave's walls at least 31,000 years ago were found paintings surrounded with numerous handprints that are felt to "have acted as an un-forgeable signature" of its originator.

- Evidence indicates that fingerprints were used as a person's mark at year 500 B.C.

- Early Chinese merchants used fingerprints to settle business transactions and also Chinese parents used fingerprints and footprints to differentiate children from one another.

- In early Egyptian history, traders were identified by their physical descriptors.

By the mid-1800s, with the rapid growth of cities due to the industrial revolution and also more productive farming, there was a bigger need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely only on their own experiences and local knowledge. Influenced by the writings of Jeremy Betham and other Utilitarian thinkers, the courts of this period began to digest concepts of justice that hold up to this day. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any

other parameter. This field was called "anthropometrics". The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualised metric - fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints (Science & (NSTC) n.d.).

Year	Description
1858	First prototype system for speaker recognition is developed
1892	Galton develops a classification system for fingerprints
1896	Henry develops a fingerprint classification system
1903	NY State Prisons begins using fingerprints
1960	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1965	Automated signature recognition research begins
1970	Behavioural components of speech are first modelled
1976	First prototype system for speaker recognition is developed
1985	Patent for hand identification is awarded
1987	Patent stating that the iris can be used for identification is awarded
1988	First semi-automated facial recognition system is deployed
1993	Development of an iris prototype unit begins
1993	FacE REcognition Technology (FERET) program is initiated
1994	First iris recognition algorithm is patented
1994	Integrated Automated Fingerprint Identification System (IAFIS) competition is held
1995	Iris prototype becomes available as a commercial product
1998	FBI launches CODIS (DNA forensic database)
1999	FBI's IAFIS major components become operational
2000	First Face Recognition Vendor Test (FRVT 2000) is held
2001	Face recognition is used at the Super Bowl in Tampa, Florida
2003	Formal US Government coordination of biometric activities begins
2003	European Biometrics Forum is established
2004	First statewide automated palm print database is deployed in the US

Table 3.1: Biometrics history.

3.9 Related Ethics Issues

There are some groups of people which are more likely to be disadvantaged by the use of biometrics as an authentication system than others. The risk is that they might be excluded from participation in society more than they currently are. Some of the groups that may be affected by the use of biometrics are:

- **People with physical and/or learning disability**

  While the use of biometrics in certain applications can be an advantage to people with some types of disability, in cases where only a limited number of people will enroll their data and the system could be fine-tuned for the individual user there are problems associated with the use of mass-verification biometrics systems. The UKPS Biometric Enrolment Trial included at least 750 disabled people and in each of the biometrics tested (fingerprint, facial recognition and iris scanning) this group did significantly worse than others in enrolling their biometrics, both in terms of accuracy and time taken to attempt enrolment and verification.

- **People with mental illness**

  No research has been published on this group of people yet, but it is very easy for everybody to assume that, for instance, some people with depressive or paranoid illnesses will be averse to using biometrics systems, with potential negative effects such as increased poverty, decreasing health, homelessness, and possibly suicide or death through conditions such as physical illness or malnutrition.

- **People of certain races**

  According to the UKPS trial, it is more difficult for black people (as they referred in the UKPS Trial Report) to enroll their facial biometric, iris, and fingerprint than other races.

- **People of certain religions**

In some religions people are required to wear head or face coverings, and so it is obvious that these people will have difficulties to enroll any facial biometrics. Verification of biometrics in public places may lead to embarrassment or offence.

- **The elderly**

  This is a group of people that is worldwide regarded generally as technophobic, and might tend to avoid any biometrics system at all, even if it is potentially helpful. According to the UKPS trial those who are over the age of 60 had more trouble enrolling biometrics, and it would not take long before confidence in using such systems was so low that people in this and other groups avoided having to use them. Considering that the elderly are more likely to need access to health and social care this could be a very serious problem if biometrics were to be used for access to social goods.

- **The homeless**

  People included in this group will face difficulties in the event of biometrics identity cards becoming a reality, given that they by definition, do not have an address to which an appointment to attend for biometrics enrolment can be sent, even if the authorities know of their existence. Even if a homeless person gets a card, the biometrics will be unreliable as such factors as health, weight loss, and cleanliness affect recognition.

The use of biometrics assumes that the data:

- can be collected
- can be verified
- and both collection and verification to be achieved in an accurate and efficient way

Even if these three rules are satisfied, the purpose of a biometrics system remains "exclusion", which means that those who do not have the right identifiers are excluded

from access to whatever is protected by it. Social exclusion is an ethical issue and can be described as "any unfair restriction or removal of access to the range of social goods and activities that other members of that society do, or could, take for granted". After all being a member of society is much more important than just access to social security.

Biometric characteristics are sensitive personal data. Whoever deals with biometrics must be very careful because a potential "robbery" of those characteristics can have many bad effects on users. Although in our case we don't have to deal with biometric characteristics at all as our main concern is to ensure the sensors integrity in a biometric-based authentication system (Wickins 2007).

Chapter 4

System Design and Implementation

4.1 Implementation Details

The implementation of this project was done with the use of java technologies. Java was used for many reasons as it has many advantages. Those advantages are:

- Java is platform-independent. This is one of the most significant advantages of Java because it has the ability to move easily from one computer system to another. The ability to run the same program on many different systems is very important to World Wide Web software, and Java succeeds at this by being platform-independent at both the source and binary levels.

- Java is object-oriented. This allows the creation of modular programs and reusable code.

- Java supports distributed environments. Distributed computing involves several computers on a network working together. Java is designed to make distributed computing easy with the networking capability that is inherently integrated into it. Writing network programs in Java is like sending and receiving data to and from a file.

- Java is multithreaded. Multithreaded is the capability of a program to perform

several tasks simultaneously within a program. In Java, multithreaded programming has been smoothly integrated into it, while in other languages, operating system-specific procedures have to be called in order to enable multithreading. Multithreading is necessary in visual and network programming.

The architecture of the project is shown in Figure 4.1. For data saving purposes only XML files were used. XML files were used in local level regarding data that each biometric sensor stores independently and also in the Database were data regarding all the sensors are collected.

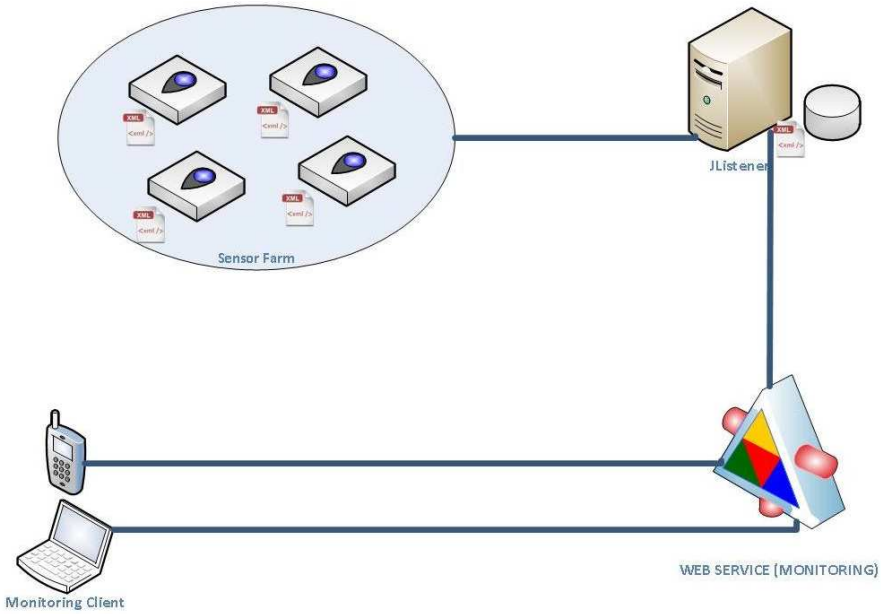

Figure 4.1: High-level architecture of developed system.

The biometric sensors (inside the "Sensor Farm" in Figure 4.1) are described with an XML file which contains the following information:

- ID: This is a unique number that is assigned automatically to every sensor added in the Database.
- STATUS: Here the status of every sensor is described. The status can be "running" when the biometric sensor is operating properly, "stopped" when the biometric sensor is out of order or "time out" when the biometric sensor sends its response with delay.

- TIMER: Here a time delay is defined in which each sensor sends its status to the server.

The sensors are represented with a java desktop application in a graphic way shown in Figure 4.2.

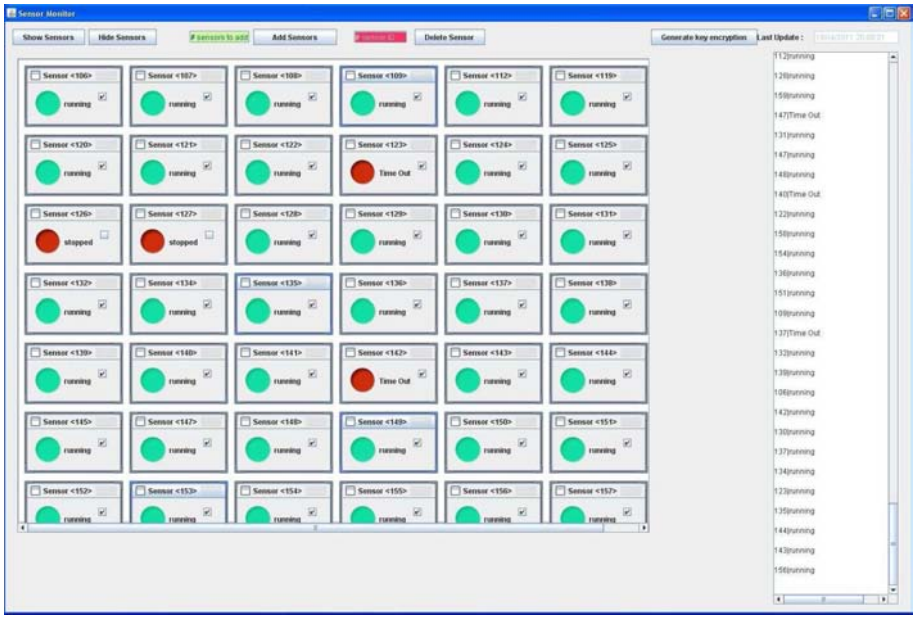

Figure 4.2: Visual display of the sensors.

Sensors with green colour work properly and have the sign "running" next to them while sensors in red colour have a problem which appears next to them either as "stopped" when they are inactive or with "Time Out" if their response was out of a time we consider accepted. In the development of the application the time that was defined as accepted was 60 seconds but that time is changeable.

This application communicates through a TCP IP socket with a Java server which was developed only for the communication with the sensors. The Java server accepts information from the sensors regarding their status, their ID and a timestamp which shows the exact date and time that the sensor sent the message to the Java server through the TCP IP port: 4444. Through this application the manager of the system can add or remove sensors and also can alter the encryption key used for the secure communication between the sensors and the Java server.

All the data collected by the Java server from the sensors are stored in the Database in an XML file called sensors.xml. There is also a Web Service which has direct access to the Database and the sensors.xml file and through this the client, no matter where he is, can take information regarding the distributed network of the sensors.

The Client application that shows the status and every possible error occurring in the sensors-network is shown in Figure 4.3.

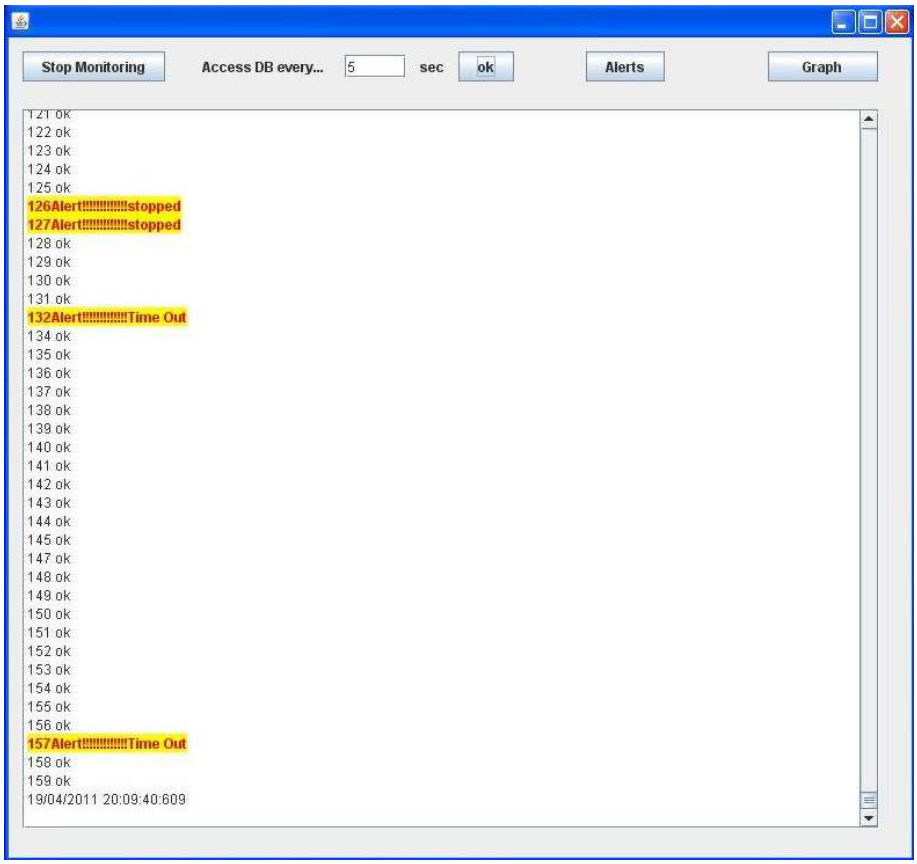

Figure 4.3: Monitoring Client.

This Client application watches and shows the status of the sensor-network "on-demand" without giving the opportunity to anyone to intervene essentially to the operation of the network and is accessible through laptops, smartphones etc. The information about the sensors-network are provided to the Client application through the Web Service.

Here there is a button called "Alerts" which shows a list with all the malfunction occurred during the monitoring of the sensors-network. This list includes the sensors id,

the date and the time the error occurred and also the exact error as shown in Figure 4.4.

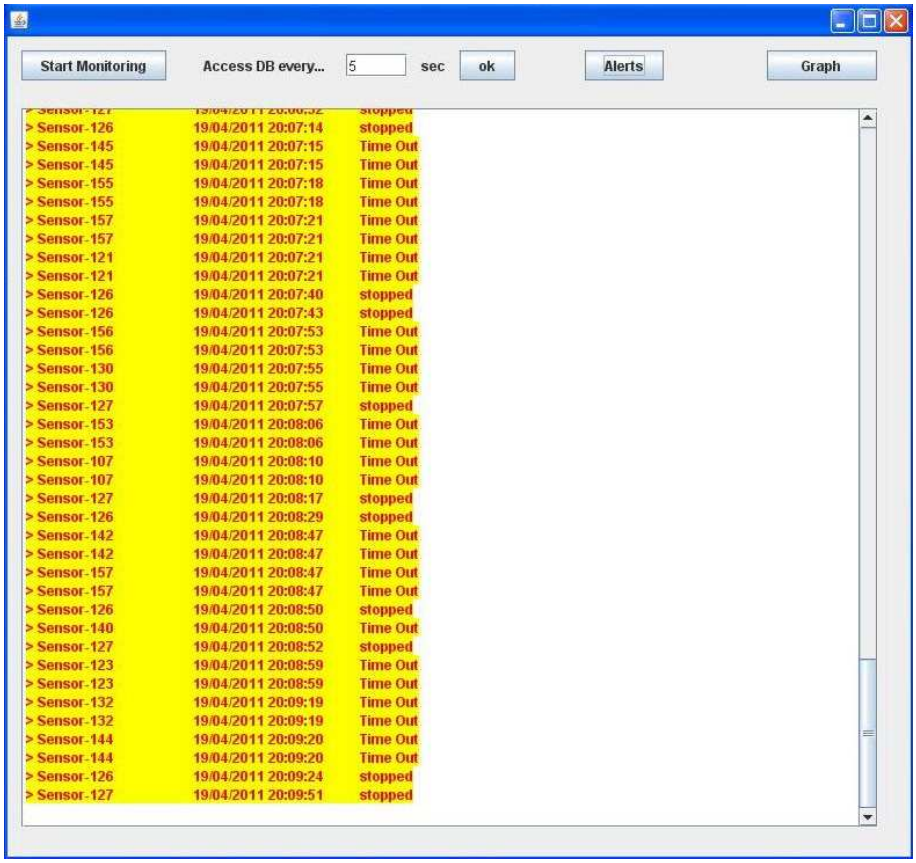

Figure 4.4: Alerts List.

In the Client application there is also a button called “Graph” which shows a graph with the number of sensors included to the monitoring with the milliseconds required to complete the scan of those biometric sensors. One such graph can be seen in Figure 4.5.

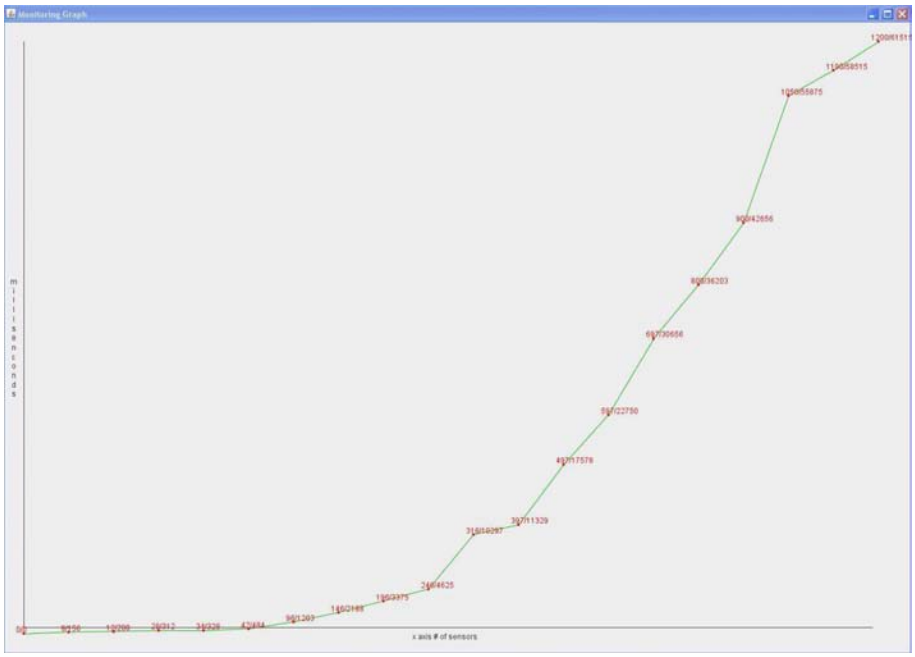

Figure 4.5: Monitoring Graph.

4.2 Security

The sensors are sending data to the java server with a secure way using the triple DES cryptography which was described earlier. The data that a sensor sends to the server are its unique id, its status and a timestamp with the exact date and time that the sensor send the package to the server. With this encryption a secure communication is achieved and several attacks can be prevented.

- Denial of Service (DoS) attacks are usual attacks in the biometric sensors and can be physical damage (like destroying a sensor by breaking it or by spilling liquid on sensors and other similar attacks) or even power loss to the system which sets the sensors out of order. If a case like this occurs the sensor being attacked will stop transmitting automatically and its status will be set at "stopped". Biometric sensors with their status set at "stopped" are instantly set as unreliable and the system is giving "alert" messages. They can be set as reliable again only manually if a technician verifies that everything works properly again.

- There are also other types of attacks that our system may have to deal with when operating. A very common attack can be the attempt of a possible attacker to steal the packet that the sensor is trying to send to the server with the method of "sniffing" or in any other way. As already stated the data that the sensors send to the server are their unique id, their status and a timestamp. Triple DES was selected as the proper encryption algorithm, in order the sensors to encrypt and send those data, as it uses long encryption keys which are very hard and time consuming to break. So for the level of security we need for the data the sensors send to the server, triple-DES encryption algorithm can provide us a confidence that even if someone steals the data he won't be able to decrypt them easily.

- In order to prevent "Replay" attacks in every encrypted packet that sensors send to the server there is a timestamp included. During the decryption the server checks the timestamp and sees when the information was created by the source. There is a specific period of time (which can is changeable according to what the manager of the application thinks is an accepted time for the sensor to send his data to the server) for the server to accept and not to reject the packet from the sensor. If the time that the message was created until the time received from the server is bigger the accepted response time, an "alert" message comes out and the system sets the sensor that hasn't reported in time as "Timed out". We can set the sensor in "running" status again manually when we get a confirmation by a technician that will check the sensor. So if an attacker tries to attack to our system by setting a sensor out of order while sending to the server one stolen packet again and again, our system will inform us with a "Time Out" message for that sensor instantly.

These are the most common attacks systems may have to deal with and the developed application is able to detect them.

Figure 4.6 shows a listener with all the communication between sensors and the server.

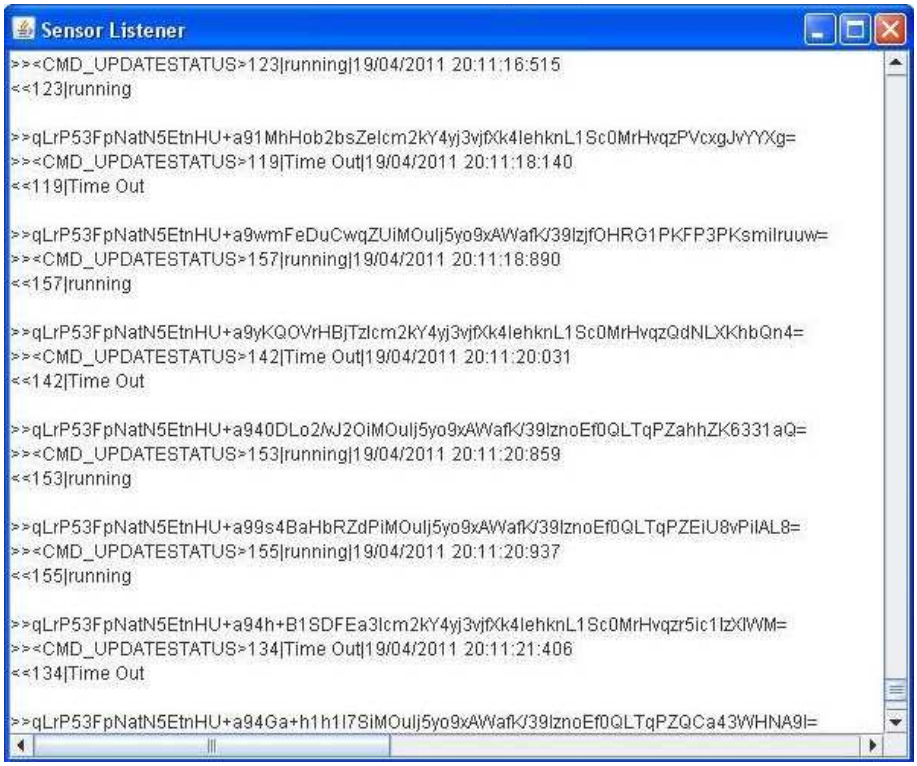

Figure 4.6: Sensor Listener.

All messages exchanged are shown in Figure 4.6 as well as the encryption key used for every message.

4.3 Results

As already stated the sensors have a specific time (which is changeable) which considered acceptable in order to send their packets to the server. If they send the packets out of that time they are marked instantly as untrusted with the sign “Time Out” next to them.

The server needs some time in order to collect all the responses from the sensors he is monitoring. Figure 4.5 shows how the time for the monitoring is changing according to the number of the sensors being monitored. Naturally the time needed for the monitoring is growing for a bigger number of sensors.

In order for the application to be functional and to operate properly the time needed

for the server to collect all the responses from all the sensors must be smaller from the accepted time that sensors have to send their data to the server. When the maximum response time for the servers is higher, then the system can operate with more sensors without problems. A graph which shows how many sensors the application can tolerate compared with the maximum response time for the sensors can be seen in Figure 4.7.

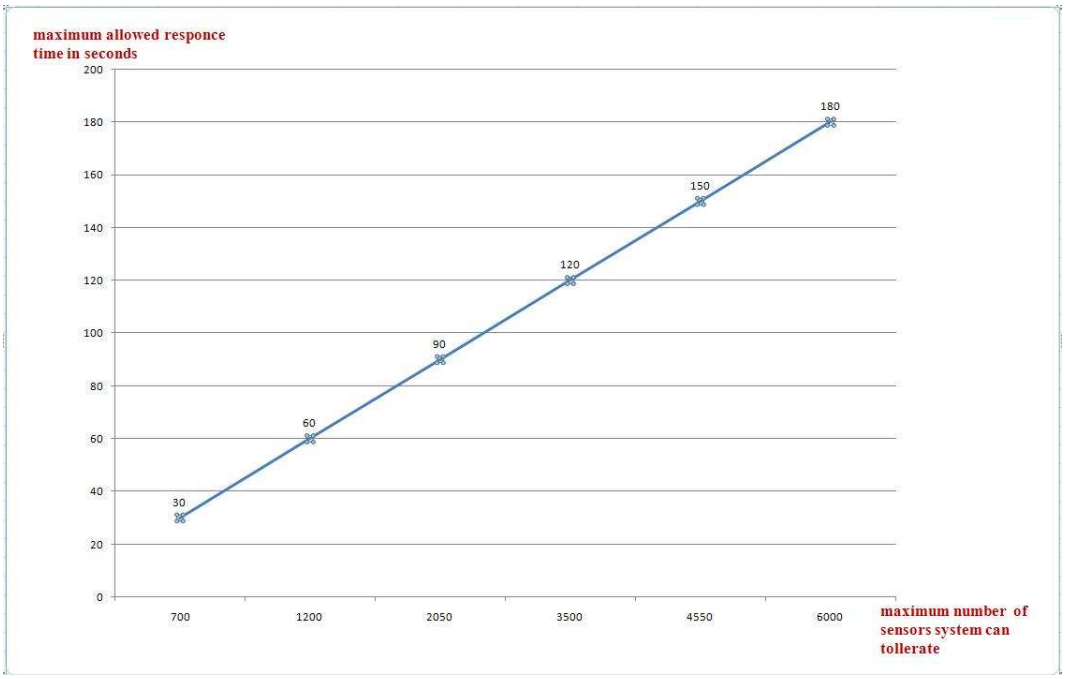

Figure 4.7: Maximum response time/Sensors system can tolerate.

Chapter 5

Conclusions

5.1 Aims of the Thesis

The aims of the thesis were at first to present a survey on biometrics and biometric-sensors and of course the implementation of an application that securely monitors a distributed network of biometric sensors. Both those objectives of the thesis were successfully delivered.

5.2 Evaluation

The implemented application is a success according to the aims of the thesis. It is an efficient and reliable application that has the security as its first priority. The data that sensors send to the server can be trusted as several attacks that might occur can be killed by the system.

5.2.1 Thesis Development

In the theoretical part of the thesis biometrics, authentication systems based on biometric characteristics, cryptography and the types of cryptographic algorithms were presented in detail. Regarding the application, it was developed in java and from

the several cryptographic existing algorithms, triple-des was the one selected for the encryption of the communication between the sensors and the server.

5.2.2 Proposed System

The java application developed for this thesis delivers its purpose of creation as it can continuously monitor any amount of biometric sensors we want being able to ensure us that they work properly at all times. Also it states any possible malfunction a sensor might have at real time giving the opportunity to the user to watch the status of the network from everywhere with the use of a Web Service. Moreover the application can defend itself from many possible attacks as sensors communicate with the server with messages encrypted with triple-des encryption algorithm.

5.3 Recommendations for Future Research

In the future the application can be even better with some changes.

- At first the triple DES which is the cryptographic algorithm used for the communication of the sensors with the server could be replaced with the AES cryptographic algorithm. AES is the current and newest standard of cryptography.
- Also an authentication system (username and password) could be added to the client in order a user to authenticate himself before he could monitor the status of the sensors-network.

5.4 Conclusions

This thesis helps in understanding what exactly biometrics are and how systems based in biometric authentication systems work. It also states some basics about cryptography that are useful for the scope of the thesis and also analyzes the different cryptographic algorithms. The application developed covers the purpose of the thesis as it

provides to the user a confidence that the sensors monitored can be trusted.

Bibliography

Chouinard, D. J.-Y. (2002), 'Notes on the advanced encryption standard(aes)', **197**.

Duke University (n.d.), 'Authentication vs. authorization', [Online]. Available: `http://www.duke.edu/~rob/kerberos/authvauth.html`.

Elliott, S. J. & Kukula, E. P. (2009), 'A definitional framework for the human-biometric sensor interaction model'.

European Commission JRC (2005), 'Biometrics at the frontiers: Assessing the impact on society', *Technical Report Series* .

Harris, S. (2008), *All-In-One CISSP Exam Guide, fourth edition*, McGraw-Hill Companies.

Matyas, V. & Riha, Z. (2002), 'Biometric authentication – security and usability', *Faculty of Informatics, Masaryk University Brno, Czech Republic* **228**, 227–239.

Olzak, T. (2006), 'Keystroke dynamics: Low impact biometric verification'.

Papanikolaou, A., Ilioudis, C., Georgiadis, C. K. & Pimenidis, E. (2008), 'The importance of biometric sensor continuous secure monitoring', *IEEE* pp. 569–574.

Podio, F. L. & Dunn, J. S. (n.d.), 'Biometric authentication technology: From the movies to your desktop'.

PRENEEL, B. (2003), Analysis and Design of Cryptographic Hash Functions, PhD thesis.

Rhodes, K. A. (2003), 'Challenges in using biometrics', *United States General Accounting Office GAO* .

Roberts, C. (2006), 'Biometric attack vectors and defences'.

Science, N. & (NSTC), T. C. (n.d.), 'Biometrics "foundation documents"', *Subcommittee on Biometrics* .

Systems, C. (2006), 'Triple-des encryption and decryption core'.

Uludag, U. & Jain, A. K. (2004), 'Attacks on biometric systems: A case study in fingerprints', *Department of Computer Science and Engineering* pp. 622–633.

VOCAL Technologies, L. (2004), 'Triple data encryption standard'.

Wickins, J. (2007), 'The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identificatio', *Springer Science and Business Media* .