ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

SMART CARD AND BIOMETRIC BASED GENERAL PURPOSE ACCESS CONTROL SYSTEM DESIGN

M.Sc. THESIS

Sercan AYGÜN

Department of Electronics and Communication Engineering

Electronics Engineering Programme

JUNE 2015

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

SMART CARD AND BIOMETRIC BASED GENERAL PURPOSE ACCESS CONTROL SYSTEM DESIGN

M.Sc. THESIS

Sercan AYGÜN
504121390

Department of Electronics and Communication Engineering

Electronics Engineering Programme

Thesis Advisor: Prof. Dr. Ece Olcay GÜNEŞ

JUNE 2015

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI KART VE BİYOMETRİK TABANLI GENEL AMAÇLI ERİŞİM KONTROLÜ SİSTEMİ TASARIMI

YÜKSEK LİSANS TEZİ

Sercan AYGÜN
504121390

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ece Olcay GÜNEŞ

HAZİRAN 2015

Sercan Aygün, a **M.Sc.** student of ITU **Graduate School of Science Engineering and Technology** student ID 504121390, successfully defended the **thesis** entitled "**SMART CARD AND BIOMETRIC BASED GENERAL PURPOSE ACCESS CONTROL SYSTEM DESIGN**", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. Ece Olcay GÜNEŞ** İstanbul Technical University	.....
Jury Members :	**Assoc. Prof. Dr. Mürvet KIRCI** İstanbul Technical University	.....
	Prof. Dr. Herman SEDEF Yıldız Technical University	.....

Date of Submission : 04 May 2015
Date of Defense : 03 June 2015

To my mother,

FOREWORD

First and foremost, I am using this opportunity to express my gratitude to all of my teachers beginning from primary school till my master's degree, especially to my thesis supervisor, Prof. Dr. Ece Olcay GÜNEŞ, who supported me both for my thesis work and my carreer plan by showing her great interest, patience and help. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M.Sc. study.

Furthermore, I would like serve my respects to Assoc. Prof. Dr. Mürvet KIRCI, Asst. Prof. Dr. Muammer AKÇAY, Prof. Dr. Osman PARLAKTUNA, Prof. Dr. Hasan Hüseyin ERKAYA, Prof. Dr. Ali TOKER, Prof. Dr. Hakan KUNTMAN, and Assoc. Prof. Dr. Berna ÖRS YALÇIN who are the important names of my master study. Besides, I would like to thank to my thesis committee for their encouragement, insightful comments, and questions.

In addition, I serve my loads of appreciation, where I work as a research assistant, to Yıldız Technical University, Computer Engineering Department for their flexibility and indulgence.

My friends, Canan Şimşek and Volkan Gezer have helped me to focus on my thesis. Their support and care helped me construct my self-esteem. I greatly value their friendship and I deeply appreciate their belief in me.

Most importantly, none of this would have been possible without the love and patience of my family. I would like to express my heart-felt gratitude to them for supporting me throughout all my studies. My mother and father, Filiz AYGÜN and Tonay AYGÜN, have been encouraging me with their best wishes all the time.

Finally, I really appreciate to Istanbul Technical University Rectorship, Scientific Research Projects Department that funded parts of the research discussed in this thesis.

May 2015

Sercan AYGÜN
Electrical-Electronics &
Computer Engineer

TABLE OF CONTENTS

Page

ABBREVIATIONS

ACS : Access Control Sytem
PC : Personal Computer
NFC : Near Field Communication
RFID : Radio Frequency Identification
PIN : Personal Identification Number
ACN : Access Node
ADN : Admin Node
UML : Unified Modelling Language
RBAC : Role Based Access Control
GUI : Graphical User Interface
EKS : Erişim Kontrol Sistemi
GÇN : Geçiş Noktası
YNN : Yönetici Noktası
USB : Universal Serial Bus
CMOS : Complementary Metal Oxide Semiconductor
HDL : Hardware Description Language
ATM : Automatic Transaction Machine
EEPROM : Electronically Erasable Programmable Read-Only Memory
MCU : Microcontroller Unit
RSA : Rivest-Shamir-Adleman (cryptosystem)
BAP : Scientific Research Projects (Bilimsel Araştırma Projeleri)
VAT : Value-added Tax
TL : Turkish Lira
USD : United States Dollar
FAR : False Acceptance Rate
FRR : False Rejection Rate
ROC : Receiver Operating Characteristic
ASIC : Application Specific Integrated Circuit
TTL : Transistor-Transistor Logic
COMM : Communication
LED : Light Emitting Diode
SPA : Simple Power Analysis Attack
DPA : Differential Power Analysis Attack
CRC : Cyclic Redundancy Check
EOP : End of Package
OOP : Object Oriented Programming
EMV : Europay, MasterCard and Visa

LIST OF TABLES

Page

LIST OF FIGURES

Page

SMART CARD AND BIOMETRIC BASED GENERAL PURPOSE ACCESS CONTROL SYSTEM DESIGN

SUMMARY

Access control systems (ACS) are the ones, which people come across frequently while entering places, passing through somewhere or even logging into any online accounts. Public transportation, authorized building or room entrance, highway passing, PC accesses, signing on to online banking or social media accounts are some examples that can be experienced during everday life as the samples of accesses. In most cases, these actions are in under control the reason why personal security plays an important role. Therefore, there are plenty of approaches and electronic systems in the literature to provide control for such cases above.

In this thesis, it is proposed an approach for low cost and easy to programme system, which is general purpose and multi-modal. General-purpose feature brings an innovation to these kind of systems to be more generic. The system can easily adapted to new applications, in other words, the system first can control door accesses, but on the other hand, it can also be used for some other applications like payment based *paypass* implementations. This diversity comes thanks to different input devices like smart card reader, fingerprint scanner, NFC/RFID reader, touchable screen for PIN entering & system response monitoring etc. Consequently, the system satisfies the multi-modal approach with these devices that make system more secure.

In the following chapters, firstly the general details of the thesis are presented in the introduction part. There are introductory information about the system scheme and some analysis that are crucial to be held previously like requirement and feasibility. Also, it can be found the hypothesis which this thesis work stands for in terms academic approaches. There is also literature review for the previously handled works. Especially for the fingerprint sensor, there are some studies that use the same device which is controlled by microprocessor.

Then, in the second chapter, the important background information for the phylosophy of this thesis is given. It contains about the preliminary explanations on behalf of biometry, cryptography, hash functions etc. Biometry is used in many different areas from security to forensic, even for diagnosis in the medicine. For authentication purposes, access systems can have sensors related to biometrics. This chapter helps the reader to understand the main frame of the study.

In the third and the main chapter, all the design issues are presented. It has basically two sub-sections. Firstly, the hardware related knowledge is described. Sensors and controllers are given in here. In this study, the system engineering approaches are used together with embedded systems; therefore, different kind of sensors are to be work synchronously via controllers. The system basically consists of two nodes: Access

Node-ACN and Admin Node-ADN. Each has a controller unit and some sensors. For the ACN, fingerprint sensor in the thesis takes the fingerprint image as 256x288 pixels in gray level. Then inside of the sensor, the whole image is transferred into characteristic file, and after into a template. There is no information related to algorithm neither in the datasheet nor in any of the source in the internet such as vendor. In our system, the data from the sensor is saved in the smart card securely and later newly captured data is to be compared with this smart card originated information. Extracted data from fingerprint must be stored securely in the smart card which does not have any extra protection mechanism. Therefore, biometric data hiding or encryption must be handled as the smart card can be on wrong hands. When access operation is needed, data in the card and the freshly read one from the user via sensor is to be compared, either does fingerprint sensor.

Moreover, in the software structure part of this thesis in the second branch of Chapter three, hardware handling software details are given in the scope of software engineering. UML diagram contains the Role Based Access Control Pattern – RBACP to give different privileges to the different users. Thesis has general purpose approach by this way. Besides, in the admin part, the Windows operating system based GUI is designed thanks to C# programming language. This monitoring screen allows admin to control the system from far. Comnunication between access node and admin node is in wireless communication thanks to XBee sensors, so communication protocol that proposed by this thesis must be secure indeed, too. As the "*access*" needs to be secure, designed system must rely some scientifically secure algorithms that thesis mainly aims at. In 1976, public key cryptography released some opportinities to make system security by key exchange. Even when two wireless devices communicate with each other, man-in-the-middle attack can be less hazardous thanks to Diffie-Hellman key exchange algorithm.

System Analysis is given in Chapter four. There are details about the system operation and some limitations related to some seperating devices that are occured during the design and the tests. All the overall system details are presented in this chapter. Any researcher who reads that thesis work can construct the system by using the hardware and software details inside. Thus, the researcher can have an ACS environment to work for security algorithms by implementation of cryptography or secure image-processing issues for future work together ciphering with fingerprint issues.

In the last chapter, last results of the project are presented. In this conclusion part, the future considerations related to thesis are introduced, too. Smart cards and NFC/RFID technology are in use for loads of applications. If the biometric information is intended to be embedded into these technologies, then some scientific questions arise related to security. Moreover, if wireless technology is in use as a hardware module, then another security circumstance emerges to be academically handled as this thesis does via design of communication protocol in the scope of Petri nets. Modelling the own protocol together with data packages, instruction codes etc. makes the thesis more academic and the system more secure. To conclude, the system was successfully designed and all academic approaches were explained in this thesis report.

AKILLI KART VE BİYOMETRİ TABANLI GENEL AMAÇLI ERİŞİM KONTROLÜ SİSTEMİ TASARIMI

ÖZET

Erişim kontrolü sistemleri (EKS) insanların belli alanlara girerken, bazı noktalardan geçiş yaparken, hatta çevrimiçi hesaplarına ulaşırken sıklıkla karşılaştığı sistemlerdir. Toplu ulaşım, yetkili bina veya oda girişi, otoyol geçişi, kişisel bilgisayar veya bulut erişimi, çevrimiçi bankacılık veya sosyal medya hesaplarına giriş, günlük yaşamda karşımıza çıkabilecek bazı erişim örnekleridir. Kişisel güvenliğin önemli rol oynamasından dolayı bahsi geçen çoğu erişim eylemi kontrol altında tutulmaktadır. Bu sebeple, literatürde çok sayıda elektronik sistem ve yaklaşım bulunmaktadır.

Genel çerçevede bakıldığında bu tez çalışması donanımsal araçları kullanıp bir araya getirerek, üzerine yazılan yazılım ile çalışan bir sistem sunmayı hedeflemektedir. Donanım parçaları tek tek anlatılacak, nasıl bir araya getirildiğinden bahsedilecek ve ardından yazılım detaylarına girilecektir. Bu sırada, yaşanan zorluklar ve sistemin sahip olduğu zayıf noktalardan söz edilecektir. En önemlisi, savunulan teze hizmet etmesi açısından sistemin içinde koşan algoritma akademik zemine oturtularak anlatılacak ve sistemin güvenliğini sağlayan yaklaşımlardan bahsedilecektir. İletişim protokolleri, komut kodları, veri paketi bu sisteme ve teze ait özel tasarımlar olup, Petri ağları da kullanılarak modellenmiştir. Böylelikle güvenlik durumları düşünülerek daha sağlam bir sistem tasarlanmıştır.

Bu tezde düşük bütçeli, programlama kolaylığı olan, genel amaçlı ve çoklu modlu bir sistem tasarımı önerilmektedir. Çoklu mod; akıllı kart, parmak izi sensörü gibi birden fazla giriş kontrol elemanının bulunmasından dolayı verilmiş bir özelliktir. Genel amaçlı olması ise bu türlü geçiş kontrol sistemlerine daha genel, farklı farklı uygulamalarda kullanılabilir bir yenilik kazandırmaktadır. Bu kapsamda sistem kolaylıkla yeni uygulamalara adapte olabilir. Örneğin, sistem önce bir kapının kontrolünü sağlıyorken, diğer yandan ödeme ile ilgili farklı uygulamalarda da kullanılabilir. Bu uygulamalar günümüzde öde ve geç şeklinde kişinin alışverişi esnasında kendine ait olan kartını kullanması ile gerçekleşir. Bu çeşitlilik farklı giriş aygıtlarının kullanılması ile sağlanmaktadır. Bu cihazlar veya sensörler farklılığı arttırarak tasarlanan sistemin farklı uygulamalarda kullanılabilirliğini arttırmaktadır. Bu cihazlara, sensörlere örnek olarak, akıllı (temaslı) kart okuyucuları, parmak izi tarayıcılarını, NFC/RFID (temassız) okuyucuları, hatta PIN girişi sağlayan klavye elemanını, sistemi gözlemlemek için dokunmak ekranları vb. verebiliriz. Bu türlü karmaşık bir sistem yaratmanın bir yararı da güvenlik ile ilgilidir. Sistemde kullanılan çoklu kontrol ve karar mekanizmaları ile tekli kontrol sistemlerine göre daha güvenli bir yapı ortaya çıkacaktır.

Tezin takip eden bölümlerinde önce genel detaylar sunulacaktır. İlk bölüm teze ait giriş bölümüdür ve temel olarak hedeflenen detaylar anlatılacaktır. Sisteme ait temel

bilgiler sunulacak olup isteri ve fizibilite gibi kritik bazı analizler sunulacaktır. Bu türlü analizler, hedeflenenler ve yapılabilirlik açısından oldukça önemlidir. Bu bölümde ayrıca hipotezden de bahsedilmektedir. Tezin akademik olarak dayandırılacağı temeller açısından savunulan hipotez önemlidir ve bu sebeple ilk bölümde verilmektedir. Hipotez özetle, "*Biyometrik sensörün, kablosuz haberleşme araçlarının, dokunmatik ekranın, akıllı kart teknolojilerinin entegre edildiği, mikrokontrolörler yönetimindeki uygulamaya yönelik bir sistemi kriptoloji yaklaşımları kapsamında akademik zeminde tasarlamaktır."* ifadesini içerir. İlk bölümde, literatür araştırması da sunulmaktadır. Daha önceden benzer konuda yapılan çalışmalara yer verilerek, bunlardan edinilen katkılardan da söz edilmektedir. Özellikle parmak izi sensörünün mikroişlemci tabanlı sistemlerde kullanılması ile ilgili literatürde bazı çalışmalar mevcuttur.

İkinci bölümde tez ile ilgili okuyucuya alt yapı oluşturması planlanan bazı önemli teorik bilgiler sunulmaktadır. Temel olarak biyometri, kriptografi gibi tezin kaynağını oluşturan konularda detaylar verilmektedir. Biyometri, güvenlikten adli uygulamalara kadar pek çok konuda kullanılmaktadır, hatta tıpta teşhis için bile kullanıldığı çalışmalar mevcuttur. Doğrulama amacıyla da zaten geçiş sistemleri biyometrik sensörler içermektir. Bu bölüm okuyucuya tezin akademik olarak dayandığı genel çerçeveyi sunmaktadır.

Üçüncü ve gelişme bölümünde tasarım ile ilgili hususlar sunulmaktadır. Bu gelişme bölümü temel olarak iki alt kısımdan oluşmaktadır. Öncelikle donanıma ait detaylar ilk kısımda yer almaktadır. Kullanılan sensörler, elektronik yapılar, kontrolcü üniteleri gibi donanımsal parçalar burada sunulmuştur. Bu tez çalışması sistem mühendisliği yaklaşımlarını kullanarak gömülü sistem uygulaması oluşturmayı hedeflemektedir. Bu sebeple değişik sensörlerin kontrolör vasıtası ile eşzamanlı çalışması beklenmektedir. Sistem temel olarak 2 düğüm noktasından oluşmaktadır: Geçiş Noktası-GÇN ve Yönetici Noktası-YNN. Her bir düğüm noktası bir kontrol ünitesine ve bazı dış birimlere sahiptir. GÇN için parmak izi sensörü 256x288 piksellik gri seviyesi değerlerden oluşan ham parmak izi verisi elde eder. Ardından sensör dâhili olarak bulundurduğu DSP işlemcisi sayesinde tüm resmi karakteristik bir dosyaya dönüştürür ve en sonda parmak izinin imzasını taşıyan şablon oluşur. Sensöre ait bilgi kâğıdında, internet ortamında veya satıcı, üretici firma desteğinde dönüşüm sırasında kullanılan algoritmalara ilişkin herhangi detaylı bilgi bulunmamaktadır. Önerilen sistemde parmak izine ait elde edilen veri akıllı kart içinde güvenli bir biçimde tutulmaktadır. Bunun için kullanılan şifreleme algoritması doğrulama sırasında kart içindeki veriyi geri elde etmelidir. Parmak izi verisi düşük hafızalı olan ve ekstra koruma mekanizması bulunmayan son derece sade bir kart içinde tutulmaktadır. Biyometrik verilerin güvenli olarak saklanması, dış ortamda kaybolma, çalınma gibi riskler taşıyan akıllı kartlardan dolayı oldukça kritiktir; kart yanlış ellerde olabilir. Erişim işlemi gerektiğinde, kartta saklı olan veri ile sensörden canlı olarak erişim yapacak kişiden alınan parmak izi verisi karşılaştırılmaktadır.

Kullanılan donanımsal parçaların ayrı ayrı olarak ve sırasıyla birleştirilerek sistemin oluşturulması hem sistem mühendisliği açısından hem de parçaların senkron çalışması açısından oldukça önem arz etmektedir. Üçüncü bölümde kurulum aşamaları detaylıca anlatılmıştır. Esas amaç, uygulamaya yönelik olan bu tezin önerdiği sistemi başka araştırmacıların da kurabilmesini ve üzerinde yine bu tezin öngördüğü üzere akademik uygulamalar geliştirebilmesini sağlamaktadır.

Ayrıca tezin ilerleyen kısımlarında, üçüncü bölümün ikici yarısında, yazılımsal yapıdan da bahsedilmektedir. Yazılım mühendisliğinin gerektirdiği tüm aşamalar tasarıma dâhil edilmiştir. Bu kapsamda UML diyagramları çizilmiş olup, yazılım deseninden faydalanılmıştır. Rol Tabanlı Erişim Kontrolü Deseni'ne sahip olan tasarım, farklı kullanıcılara farklı öncelikler tanımak için bu yapıyı kullanmaktadır. Bu şekliyle tez "genel amaçlı" başlığını desteklemektedir. Yönetici tarafında, Windows işletim sistemi üzerinde çalışabilecek kullanıcı arayüzü tasarlanmıştır. Bu kullanıcı dostu arayüz C# programlama dilinde oluşturulmuştur. Bu izleme arayüzü yöneticiye sistemi uzaktan kontrol etme imkânı sağlamaktadır. Erişim noktası ve yönetici noktası arasındaki haberleşme kablosuzdur, bu sebeple haberleşme protokolü güvenli olmalıdır. Girişin güvenli olması için, tasarlanan sistemin bilimsel olarak güvenilir algoritmaları kullanıyor olması gereklidir. 1976 yılında açık anahtar kriptografisinde meydana gelen gelişme, güvenli anahtar değişimini sağlamıştır. Buna göre günümüzde hala kabul gören Diffie-Hellman algoritması sayesinde arada adam saldırısı gibi kablosuz haberleşme sırasında ortaya çıkabilecek saldırıların riskleri de azaltılmıştır.

Güvenlik, yalnızca başkaları tarafından önerilen algoritmaları kullanmakla değil, ayrıca bu tez ile akademik olarak önerilen yeni bazı yaklaşımlarla sağlanacaktır. Bu kapsamda haberleşme protokolleri bu çalışmaya özel olarak modellenmiş ve kullanılmıştır. Petri ağları yardımıyla modellenen haberleşme protokolü sözde kod ile de gerçekleme aşamasından önce hazır hale getirilmiştir. Bu çalışmaya ait olan özel iletişim paketi ile yeni veri formatı güvenli haberleşme sağlamıştır.

Dördüncü bölümde sisteme ait bazı analizler sunulmaktadır. Sistemin çalışmasına ve bazı kısıtlara yönelik detaylar bu bölümdedir. Kısıtlar, tasarım ve test aşamasında ortaya çıkan, çoğunlukla donanım kaynaklı olumsuzluklar olarak nitelendirilebilir. Sistemin çalışmasına ait tüm detaylar da bu bölümde yer almaktadır. Amaç, tezi okuyan bir araştırmacının benzer bir sistemi kolayca kurmasını sağlamaktır. Bu sebeple tüm donanım ve yazılım detayları paylaşılmaktadır. Böylece, araştırmacının kriptoloji, güvenlik, hatta güvenli görüntü işleme gibi konularda çalışabileceği bir geliştirme ortamı sağlanacaktır. Güvenli biyometrik görüntü işleme gibi konular tezin gelecek çalışmaları olarak öngörülmektedir.

Son bölümde, elde edilen son sonuçlar sözel olarak vurgulanmaktadır. Bu kapanış bölümünde, gelecek çalışmalardan da bahsedilmektedir. Temaslı akıllı kart ve NFC/RFID teknolojileri pek çok uygulamada kullanılmaktadır. Eğer biyometrik veriler bu kartların içine gömülmek istenirse bilimsel bazı güvenliğe ait soruların sorulması olasıdır. Dahası, eğer kablosuz haberleşme teknolojisi de donanım modülü olarak yer alacak ise kontrol edilmesi gereken başka bir güvenlik açığı daha doğmaktadır. Bahsedilen güvelik durumları tezin gerçekleştirdiği üzere akademik olarak çözülmelidir. Sonuç olarak, hipotezi sağlayan ve donanımsal olarak doğru çalışan, iyi tasarlanmış yazılım barındıran bir bitirme tezi ve uygulaması elde edilmiştir.

Yapılabilecek gelecek çalışmalar olarak ise yüz tanıma teknolojisinin bu sisteme entegre edilebileceği söylenebilir. Özellikle stenografinin de gelişmesi ile şifrelenmiş yüz şablonları ADN tarafındaki RFID kart içine gömülerek sistemin hem çoklu mod biyometriyi desteklemesi hem de güvenliğin bir kademe daha artırımı sağlanabilir.

1. INTRODUCTION

Access Control Systems are in widely use and open to be developed in terms of increased security, response time, ease of use such as user-friendly interface, multi-modal sensory approaches etc. This thesis aims to introduce a whole system from hardware to software together with some applied algorithms such as security related ones from cryptography.

During our daily actions, we come across many different access systems that should provide protection for public. These systems should be mechanical turnstiles, electronic lock based doors or some cyber systems that you access via your personal information. All of these systems have the common critical issue: "*security*". Unwanted people should access your place or system by just masquerading as you. These people or hackers in other words, can damage your system, stole your information or belongings. In todays' access systems, many different hardware and software solutions are in use to construct more secure versions. Biometric based sensors or methods and personal identification card based systems are the ones frequently used in reliable systems. Even more, as used in mobile phones, PIN is other well-known criteria to lock your data. As technology develops, there becomes some other needings to support new developments. For example, biometric sensors that are used in access systems bring the issue how to provide biometric data secrecy especially if there is a usage of card-based system security. All in all, the whole design steps are required to be implemented for the following researches by using modelling languages and some standards.

1.1 Purpose of Thesis

In this thesis, it is also aimed to add more scientific meaning into the development kit based applications. Some algorithms are considered to be applied into these hardware electronic of things by bringing some proposed improvements into the literature. Arduino microcontrollers are up-to-date technology that serve easy-to-program

features mostly in C/C++. I/O pins also allow the coder to be as free as possible to choose the input and output devices.

Scientifically, this thesis proposes the low cost, secure, smart card and biometry based general-purpose access control system for entrants and for the admin. The chosen microcontrollers has low memory, the reason why software design of the proposed system must be as possible as efficient. Furthermore, security issue must be considered both for biometric data hiding and for the wireless communication between nodes. There are basically two nodes to be constructed: Access Node-ACN and Admin Node-ADN. They are going to communicate with each other in a secure way. Public key cryptography is to be applied for wireless communication and by that way a secure algorithm, Diffie Hellman Key Exchange, is going to be realized in an electronic system. Thus, proposed system is going to be more resistant to possible attack scenarios as in Figure 1.1. In this general form, while the communication between Alice and Bob, there can be someone else as a third person, Eve, who tries to listen them.

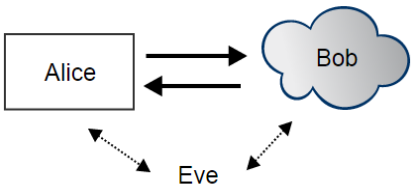

Figure 1.1 : Possible attack scenario for any system.

This project combines some different input devices to work synchronously via the microcontrollers. Therefore, hardware structure and software structure of the thesis is aimed to be presented in details. Besides, system engineering approaches are to be used the reason why system level modelling needs some steps like requirement analysis, feasibility analysis, use-case scenarios and diagrams, UML diagrams, UML sequence diagrams etc. which help to construct a robust, reliable, and secure system. At the end, a working system that supports biometric issues and cryptographic security approaches is targeted.

1.2 Hypothesis

The proposed scientific approach that distinguishes this thesis work from the others is introduced in this part. In system design, there are several ways & methods to create the whole system. One can be low level design in terms of CMOS technology, the other can be one step further that programming the related transistors in the gate arrays, HDL, one another can be the microprocessor or microcontroller based design to consider I/O devices to construct whole system with programming issues as the vital part of the embedded systems. In this thesis, it is proposed to serve a properly working system in which hardware that applies some scientific approaches in terms of security via its software design. By the hardware systems to be constructed, all of the sensors are expected to work synchronously such as Synchronous Serial Communication. The security for biometric data can also be handled by data hiding in smart card.

In a short explanation, it can be given the hypothesis as: *''Modelling and designing an application dependent multi-modal sensory system, to realize Admin – Access node based control environment, with all synchronously working sensors that satisfies secure wireless communication by handling a cryptography algorithm for enhanced security and writing down protocols satisfies all of above.''*

Moreover, this thesis proposes to give more scientific meaning in to an application based project that is uprising trend in engineering. To achieve this, some standards can be used like use case schemas, UML diagrams, patterns for software design, UML sequence diagrams for the whole system working structure, etc. In this system design application thesis, one another approach is to create a high level layer to distinguish user from microcontroller level by serving a GUI that user just interact with the interface for the access or admin operations.

High level of abstraction
C/C++/C# level of the design
Microcontroller
Assembly Language
Machine Code

Figure 1.2 : Possible layers of an electronic system.

1.3 Literature Review

This thesis is proposing an application based design; hence, mostly the journals related to engineering applications were reviewed. In this review section, it is tried to gather previously completed academic works by citing them.

Historically, access control was based on some primitive methods like someone detecting some else's face. Then, more technological way "*primitive key locks*" substituted this costly method. Whereas, the valid key can be on the wrong person and this does not mean that *owner=authority*, which still has effect on today's access controls [1]. It is forecasted about the future in 1989 that there will be developments about biometrics and smart cards as drawn in Figure 1.3.

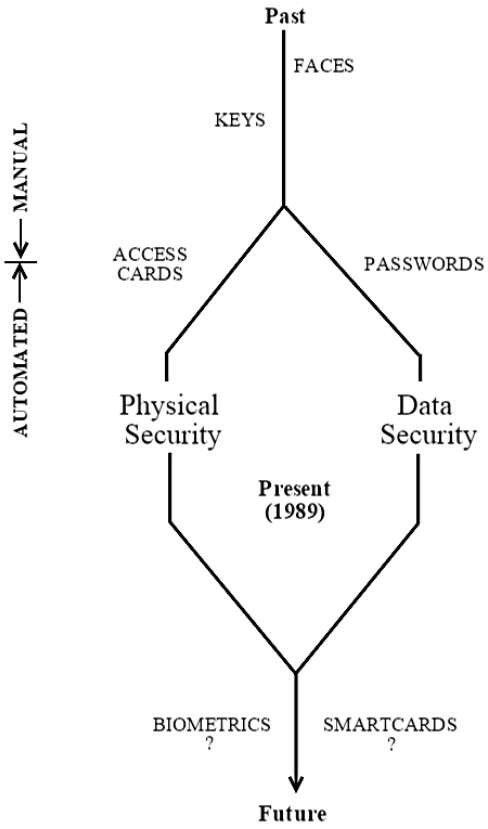

Figure 1.3 : Historical trends of access control and identity verification [1].

In the Figure 1.3, the Driscoll et al. serves the historical trends of security system by trying to foresee the future, in other words, it can be thought that future in that time is understood as "now" which points 2015 technology by underlying the biometrics and smart cards to be used in access systems [1].

If it comes to application together with theory, first of all, one of the recent work for the fingerprint based biometric ATM authentication system was handled by Sunehra [2]. He proposes a system that is microcontroller based prototype of ATM cash box access system with fingerprint sensor. Especially for the used fingerprint sensor device in the system has many features in common compared to this thesis work. On the other hand, Sunehra does not develop any biometric data securing related applications.

During the design of a system, some terms is underlined as critical points to be resolved such as *Usability, Adaptability, Credibility,* which are the basic criterion for these kind of systems while testing their success [3].

The idea to combine biometric information together with smart card technologies was also used by Abdullah et al. [4]. Chen and Yeh proposes an access control scheme by using smart cards. They explain Chien-Jan's scheme in their work to be applied between user-server communications. Importantly, for the registration phase of their own proposal, it is explained how to embed data into the smart card with an attack resistive approach [5]. *Registration*, *login*, and *authentication* are the phases seen in the literature during card based access systems which match the most in the proposed system [6]. In one of the detailed research on behalf of fingerprint sensor which is the same on this thesis is used, too [7]. In the literature, an indicating study conduct how to produce hash values from the fingerprint data. As known, hash functions' output values is very depended to the input. Even if one bit changes, the result completely changes. Therefore, securing fingerprint data by hash functions require some error handling. This approach is called symmetric hashing that [8] explains well. Tulyakov et al. present following equations for flexible biometric data hashing. Equation 2 and 3 are the possible inputs for Equation 1, which substitutes the same results. This shows the flexibility of this mathematical approach that can be referenced in this thesis, too.

$$H^m(x) = x_1^m + x_2^m + \ldots + x_n^m \quad \textbf{(1)}$$

$$X = x_1, x_2, x_3, \ldots, x_n \quad \textbf{(2)}$$

$$X = x_2, x_3, x_n, \ldots, x_1 \quad \textbf{(3)}$$

In this thesis, similar approach is followed by choosing the key for the user which also solves randomizing problem in computer science. Following equation is the way to implement it instead of *rand()* functions.

$$H^m(x) = (x_1 + x_2 + \cdots + x_n)^m \quad \textbf{(4)}$$

In Section 4, this formula is recalled to be used for fingerprint data comparison. Every x value can carry information related to the polar coordinates of the fingerprint minutiae points, from that idea the formula is considered to be applied.

In the literature, there is also another approach for biometry based systems related to multimodal biometric sensors work together. One study uses multi biometric data from single user to get all of them into one entity, which is then secured via fuzzy vault framework [9]. By this study, Nandakumar and Jain underlines the importance of template security in biometry, too. One another study from Jain et al. examines the biometric template security by combining fingerprint data securing and cryptography together. It is also analyzed some attacks like *Hill Climbing Attack*. In the paper, it is also concluded that smart card fashion is increasing which some state-of-the-art smart cards have 64 Kbyte EEPROM memory that make them more risky for biometric template misuse with large informative data [10]. While, this thesis work uses 256 Byte memory that is the equal amount of memory according to fingerprint sensor template data. Jain and Uludağ introduce a technique to embed any biometric information to one another in the scope of stenography.

On the other hand, using microcontroller unit (MCU) for cryptography is a tough problem the reason why low performance hardware structure does not support long bytes of data types i.e. at most 32 bits for unsigned long, long and float. If there is not a special crypto shield in the system or another solution via software to combine multiple variables to reach many bytes like 512 bits, it is needed to use the 32 bits for key operations. In the literature, there is a proposal to use MCU for RSA cryptosystem which is useful for small scale networks [11].

1.4 Requirement Analysis

Every project needs to meet some specifications. These requirements are application dependent and can diverse the whole system. In this thesis, the required specifications are also defined by looking at the market and defining the frames of the project. By obeying the budget, components had to be chosen as cheap as possible which are also enough efficient to implement the requirements. Moreover, there are some targets in terms of academic purposes to complete like realizing some algorithms properly by

using the hardware structure. System engineering requires defining requirements previously that help to draw the route both for the designer and for the customer if the system is a demand by a customer. It is better to write down the details of the project even with natural speaking language like doing brainstorming, but then next phase of the design requirements are transformed into use-case schemas. Following Table 1.1 is for the list of some specifications that this thesis must satisfy.

In the manner of software engineering, on behalf of interdisciplinary approach, software design issues get resistance as the design evolves or software life span progresses. Changes in the late phases of the design is hard to implement by the designer. Even the cost exponentially increases as the design proceeds. Therefore, requirement analysis must be comprehensive.

Table 1.1 : Required features supplied by our proposed system.

Required Features of the ACS
-There will be two control units. Each has some sensor(s) on it.
-Sensors will synchronously work and their interfaces will be implemented.
-The microcontrollers will be communicated via wireless sensors.
-There will be some users to access and at least one admin to monitor the system.
-There will be at least two nodes: Access Node and Admin Node.
-Access part of the system authenticates the users by using fingerprint information, smart card, personal identification number.
-Users can have different privileges as the general-purpose specifications of the thesis demands, but for demo this can stay on design level.
-Admin can monitor access part of the system, for each access demands.
-Admin part of the system will be connected to a PC with desktop application.
-Wireless communication between nodes will be handled in a secure way.
-Smart card holds the biometric data of the user who cannot infer any meaning from it.
-The user friendly GUI, both for admin and the user who has access operation will be implemented.
-Access node of the system will have a touch screen based GUI
-Admin node of the system will be linked to the Windows running desktop GUI.

The required features are to be supplied during the project proposal to choose the components of the system properly. This thesis is financially supported by Istanbul Technical University Rectorship, Scientific Research Project Department (*İstanbul Teknik Üniversitesi, Bilimsel Araştırma Projeleri Birimi, BAP*), therefore it has a budget to be considered with the limitations. As a matter of fact that the project is even stand for a low cost design for the upcoming scientific researches.

1.5 Feasibility Analysis

Feasibility analysis for this project had been held at the very first steps by considering the market and the recent necessities. Authorities in some countries decided to pass a law that national identities should be in the form of smart cards, which carry some biometric information. Also in Turkey, the situation will be the same and the whole country will have had the new smart ID cards by 2016 as the officials say. Therefore, the components to integrate a system are needed to be cleverly chosen that satisfy the general expectations. For the example previously given about some countries above, there should be intelligently decided devices and accessories to meet the need. For instance, the amount of a card memory will affect the type of the smart card or the sensors that check some other biometric specialities will diverse the whole system. Vein readers, retina scanners, fingerprint sensors, or some other cards like RFID, NFC etc. will add more hardware and software load into the access system. Then, a crucial trade-off occurs that whether the aimed project is possible to be achieved or not.

Furthermore, feasibility of hardware construction part of the project requires sensor – controller compatibility, together with sensor – sensor synchronization. System structure contains some shields to controller card for less wiring, but the other attention must be paid for pin overlaps. As an illustration, some serial communication pins of the different sensor shields can use the same serial communication channel, and then the designer must move one sensor connection to one another channel. Even more, power consumption issue must be considered depending on the where the whole system will be constructed. Before anything else, the project budget as in Table 1.2 must be taken into account. By considering all requirements, components were purchased as in the following table.

Table 1.2 : Costs of the each element in the system*

Element Name	Quantity	~Cost (without 18% VAT)
Arduino MEGA ADK	x1	186 TL
Arduino UNO	x1	40 TL
Fingerprint Sensor	x1	180 TL
XBee Module 2mW Series 2	x2	123 TL
LCD (with accessories)	x1	318 TL
Smart Card Reader	x1	22 TL
Smart Card	x1	2.7 TL
XBee Shield	x2	91 TL
NFC/RFID Module	x1	86 TL
NFC/RFID Tag Accessories	x1	22 TL
		+----------
	TOTAL:	~1071 TL

*by the purchase date 07/08/2014

As can be seen, the total cost of the system is approximately 1071 TL (496 USD), which obeys the rule of low cost budget. Accordingly, in the market these kind of systems are far beyond of this numbers, therefore low cost aim is achieved.

2. BACKGROUND

In this chapter, the basic principles and theoretical information about the thesis will be given. Biometry and cryptography are the key topics in this thesis to be explained. For the ease of understanding following chapters, this background details guide to the reader.

2.1 What is Biometrics?

Biometrics term phonetically means “life measurement” that stems from Greek words bios (life) and metron (measurement) [12]. Biometric features have been employed since years for criminal researches to identify the guilty people. Even more, last identification approaches like in passport control points use the biometric features.

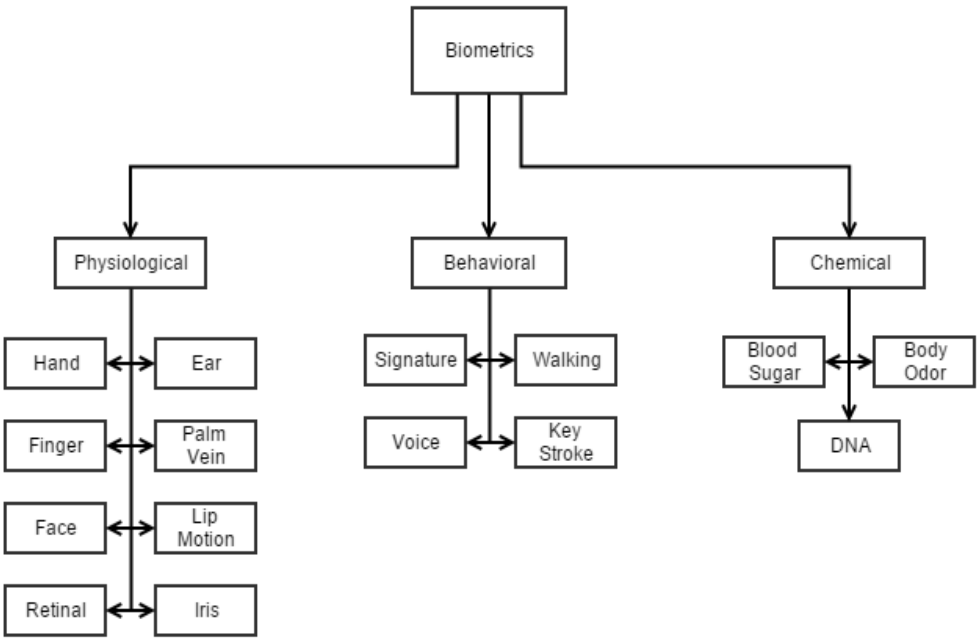

Figure 2.1 : Classification of biometric methods [13].

Depending on the physiological, behavioral, and chemical features, biometrics can be classified in terms of the methods as illustrated in Figure 2.1 [13]. Before the biometry based applications and designs, this classification would be used to decide sensor types.

Table 2.1 : Comparison of biometric technologies [14].

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 2.1 serves the comparison between biometric identifiers. In the table, high, medium and low sides of the identifiers are given by Uludağ et al. By looking at the table, it can be inferred that the fingerprint biometric identifier has no low side effect like hand geometry and many sides of it in high, especially like performance accordingly. Additionally, a survey presented in [15] shows that fingerprint biometric approach is much popular and seems much secure for survey participants. Therefore, in the proposed system of this thesis, there is fingerprint sensor by considering all of above.

Privacy preserving techniques in biometrics are the vital researches, because user security and secrecy are very important. Biometric information cannot be on the malicious hands, so that it needs to be hidden by scientific approaches. In the literature, there is an approach, which is called *cancellable* biometrics to transform biometric data into obscure version that malignant people or cyber systems cannot make deduction from biometric data.

In general speaking, biometric-based systems have two steps. One is *enrollment* that the user of the system must register with his biometric data, and the second *verification*, that using same biometric information user has to prove his identity [16]. Depending on these actions several times, some analysis can be driven by using biometric metrics.

2.2 Biometric Performance Metrics

Biometric systems are to be analyzed in terms of their success. As in data & knowledge engineering standards, some terms define the boundary of the system performance. Yet, it defines the reliability of the overall system.

The designed system with biometric sensors, or applied image processing techniques for biometric identification is needed to be considered in terms of data and knowledge engineering. Several performance metrics analyze proposed design with scientific manner. Here are the basic metric terms [17]:

- **False Acceptance Rate - FAR (or false match rate - FMR):** This is the measure of incorrectly accepted inputs even though there is not such a pattern in database like the input.
- **False Rejection Rate - FRR (or False Non-Match Rate - FNMR):** If the incoming pattern is rejected even though the database has the the one.
- **Receiver Operating Characteristic – ROC (or Relative Operating Characteristic)**: The ROC is a kind of trade-off between FAR and FRR can be illustrated via graph. "*Algorithm related to matching of biometric template does perform a decision based on a threshold, which determines how close to a template the input needs to be for it to be considered a match*" [17]. In data mining, it can be calculated via the ratio between true positives and false positives.

2.3 Why is Multi-Modal?

The recent technologies allow researchers and engineers to use loads of different sensors for different system level modelling projects. Especially for the security related systems, there can be some drawbacks to use only one type of sensor. Sensor in here

must be any type of biometry-based sensors like fingerprint, or the card based system like in payment systems or any of portable card technology related ones like RFID, NFC as contactless or else contact smart cards. The term multi-modal underlines the importance of collating some advantages of different technologies where it helps to eliminate every single sensor's disadvantage while boosting each sensor's own characteristic benefit that absorbs others.

Beverly L. et al. claims that for sensing human activity by sensors is obtained better in accuracy and practicability when the multiple types of sensors are used [3]. Moreover, Anil Jain et al. introduce a new biometric system that has three different biometrics; fingerprint verification, face recognition, and speaker verification. It is proposed that some limits stem from single biometrics are eliminated and reliability is increased by such an integrated system [18]. JuCheng Yang proposes that the minutiae-based fingerprint systems can lead some non-robust examples because of injured fingers, which can be fed by some other sensors [19].

In this study, it is proposed that multi-modal system is far better than others and all the communication of hardware devices are in the frame of secure communication. Therefore, not only the one sensor or several from the same taste, but different technologies that are in the construction of the system. Even more, multi-modal system can easily handle identical twins biometric data similarity problem for security and disabled people position in the case any damaged biometric data demanded from them. For this study propose, following Figure 2.2 and Figure 2.4 illustrate the multi modes of authentication for ACN and ADN respectively.

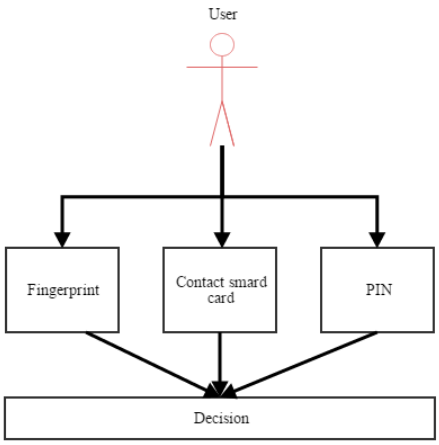

Figure 2.2 : User multi-modal authentication for new access.

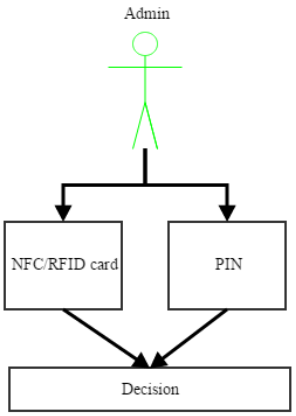

Figure 2.3 : Admin multi-modal authentication.

2.4 Cryptographic Approaches

Security related projects surely require cryptography to be applied. Therefore, it is better to present tuples of the secure system. Cryptosystems have the five following tuples: $\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$

• $\mathcal{P}$: plaintext space.

• $\mathcal{C}$: ciphertext space.

• $\mathcal{K}$: key space.

• For each K ∈ $\mathcal{K}$, there is an encryption rule eK ∈ $\mathcal{E}$ and a corresponding decryption rule dK ∈ $\mathcal{D}$. Each eK : $\mathcal{P} \rightarrow \mathcal{C}$ and dK : $\mathcal{C} \rightarrow \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every element x ∈ P [20].

Plaintext space is where the message that is going to be encrypted by using key space and the ciphertext space is the set that the encrypted message remains.

2.4.1 Diffie-Hellman key exchange

During the communication between two people, Alice and Bob, the secure key distribution must be handled for authentication purposes. Alice and Bob have private keys each to be secured and isolated from every one. Whereas, the secret key would be transferred towards the opposite side to be communicated. Alice has a and Bob has b as private numbers for illustration. Moreover, there are two more parameters to secure these secret keys: α and p. Diffie and Hellman propose an algorithm by using exponentiation and modular approach.

According to Equation 5, each *a* and *b* processed exponentially first by α and then mod *p*. They are now ready to be sent.

$$(\alpha^b mod\ p)^a\ mod\ p = (\alpha^a mod\ p)^b mod\ p \qquad \textbf{(5)} \quad [21]$$

In the opposite side, the secured keys have the same math operations and the result should be the same to guarantee the authentication. Figure 2.4 gives details about theory.

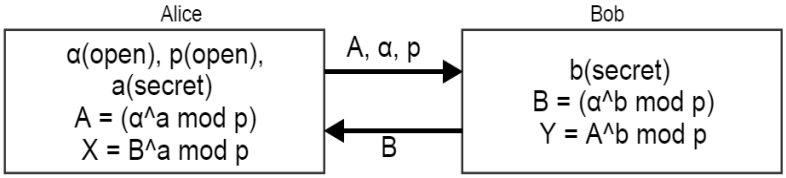

Figure 2.4 : Diffie Hellman Key Exchange Algorithm [22].

Following case study with small numbers, clearify the aforementioned method.

Case Study:

$$\alpha = 5,\ p = 7,\ a = 2,\ b = 3$$

$$5^3\ mod\ 7 = 125\ mod\ 7 = 6\ = (\alpha^b\ mod\ p) = B \text{ and}$$

$$5^2\ mod\ 7 = 25\ mod\ 7 = 4\ = (\alpha^a\ mod\ p) = A$$

According to Equation 5,

$$(\alpha^b\ mod\ p)^{\ a}\ mod\ p = (\alpha^a\ mod\ p)^{\ b}\ mod\ p$$

$$= (B)^a\ mod\ p = X = (A)^{\ b}\ mod\ p = Y$$

$$= (6)^2\ mod\ 7 = (4)^3\ mod\ 7$$

$$= 36\ mod\ 7 = 64\ mod\ 7$$

$$= 1 = 1$$

$$X = Y$$

is obtained.

In this study, Diffie Hellman key exchange will be realized in hardware, which is especially crucial for wireless communication between nodes.

3. SYSTEM DESIGN

3.1 Hardware Structure

The system is expected to fulfill some requirements that are explained previously. Depending on them, at the very early phase of the design, the elements in the system are decided.

There will be two nodes in the design for ACS illustration purpose. One is the admin node, which is possibly the unique, and the other is the access point that the users pass/access/log in. The access node can be increased depending on the application. In this thesis, illustration is handled via only one access node.

System design projects are expected to satisfy some conditions that there is an approach (algorithm) for a specific application, which is to be realized in the hardware. This trend supports the ASIC design, too.

Following sections include the system element details, their integrations steps, and synchronization issues both for hardware and software structures. Next, employed elements in the system one by one is introduced with their details.

3.1.1 Elements in the system

In the following subsections, all the elements from microcontroller to sensors in the system will be introduced. These devices construct the access node and admin node.

3.1.1.1 Arduino MEGA ADK

Every system has at least a unit for control operations. In computers and computer like systems, there is a CPU to handle some operations via ALU and control unit. All of the organizations of these units together with shifters, registers, buses, clock etc. are handled and related instructions are processed. In our system, there are two control units for access and admin monitoring. Arduino MEGA ADK (ATmega2560) supports multi serial ports totally four, the reason why it is nominated for the proposed system. It is presented in Figure 3.1.

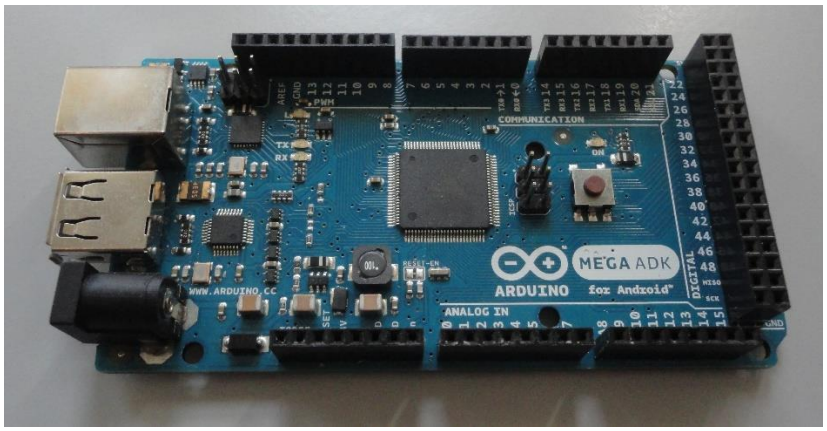

Figure 3.1 : Arduino MEGA ADK.

The basic features of the controller of access node are given in Table 3.1.

Table 3.1 : Arduino MEGA ADK features [23]**.**

Feature	Values
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	54 (15 PWM output)
Analog Input Pins	16
DC Current per I/O Pin	40 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	256 KB
SRAM	8 KB
EEPROM	4 KB
Clock Speed	16 MHz
USB Host Chip	MAX3421E

3.1.1.2 Arduino UNO

The admin part of the system has Arduino UNO (ATmega328). It has less pins and features, plus it has a chip on it which can be removed to be used somewhere in a printed circuit board for own designs. UNO is a cheap microcontroller and has low memory. It is shown in Figure 3.2.

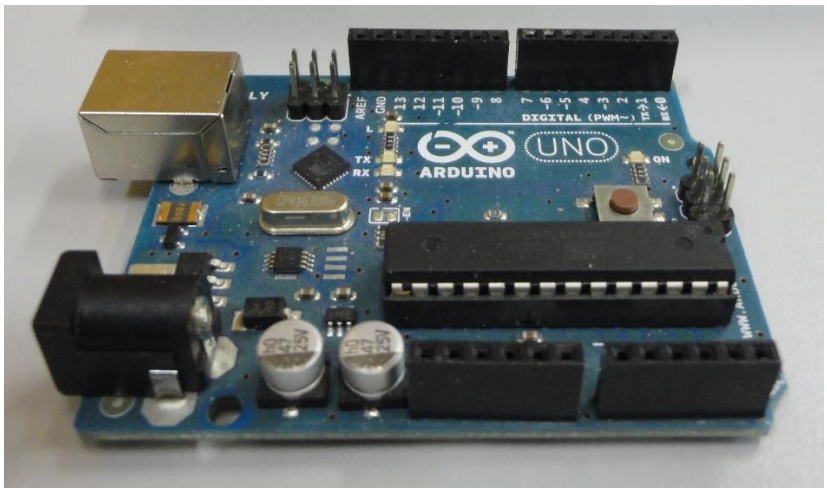

Figure 3.2 : Arduino UNO.

The basic features of the controller of admin node are given in Table 3.2.

Table 3.2 : Arduino UNO features [24].

Feature	Values
Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	14 (6 PWM output)
Analog Input Pins	6
DC Current per I/O Pin	40 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB
SRAM	2 KB (ATmega328)
EEPROM	1 KB (ATmega328)
Clock Speed	16 MHz

3.1.1.3 Smart card reader/writer

One of the accessories in this study is the smart card reader. It helps to read and write the embedded data in the smart cards, which carry information. In the smart card reader module, which is from Parallax Company, there are six pins to be used. The model that was chosen is for memory-based smart cards and not compatible with the microprocessor based ones. Table 3.3 shows output pin names. The reader actually can do the writing operation easily, which is crucial for the system of thesis during new user enrolment. Figure 3.3 and Figure 3.4 shows the details of the pins for smart card module.

Table 3.3 : Smart card reader/writer module pin definitions [25].

Pin	Name	Type	Function
1	I/O	In-Out	Bidirectional data I/O
2	CD	Output	Detects whether card is inserted
3	CLK	Input	Synchronous clock input
4	RST	Input	Reset
5	Vcc	Power	Supply voltage
6	GND	Ground	Ground

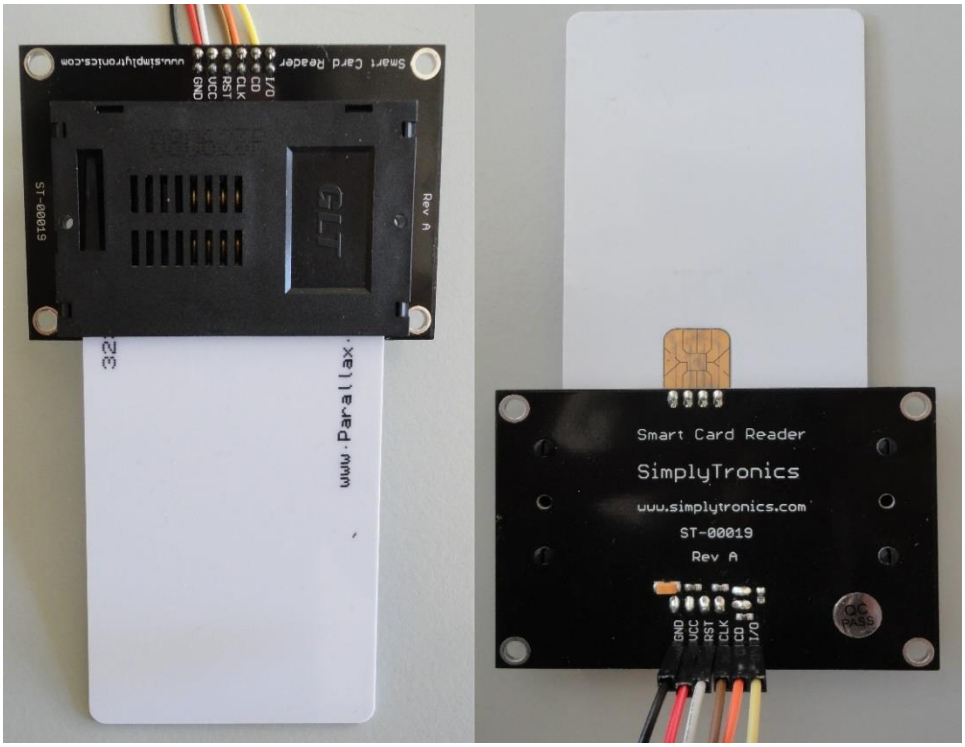

Figure 3.3 : Parallax smart card reader module.

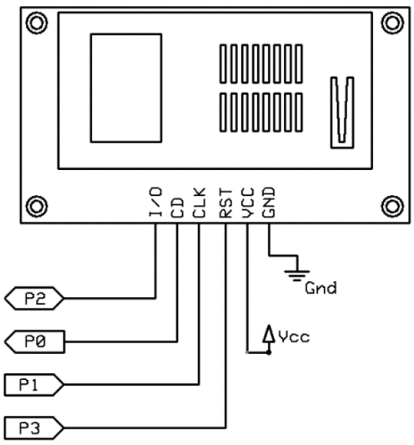

Figure 3.4 : Parallax smart card reader module with detailed pins [25].

Smart cards are also required to write data inside in a secure way. This smart card reader company serves also three types of card to be purchased. Two of them are without any extra 3-byte programmable security code and 3-bit error counter. One has 2 KB serial EEPROM memory and the other has 256 bytes. Last type has low memory and does not have any extra security bits. In this thesis, the former type of the 256 bytes memory, insecure one is chosen to implement low memory handling and creating own security approach in the sense of academic approaches as underlined in thesis hypothesis. The chosen IS24C02A Smart Card – 32323 is shown in Figure 3.5. It communicates via I^2C (CMOS) communication type.

Figure 3.5 : Parallax smart card IS24C02A Smart Card – 32323.

This pocket-sized contact card has the pad layout as in Figure 3.6.

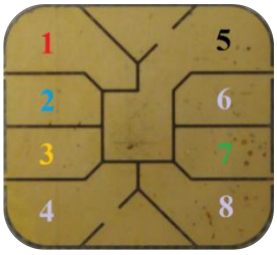

Figure 3.6 : Chosen smart card pad layout.

The aforementioned smart card pin details are given in the following Table 3.4.

Table 3.4 : Contact smart card pad definitions.

Contact Number	Name	Function
1	Vcc	Supply voltage
2	RST	Reset
3	CLK	Synchronous clock input
4	NC	No connect
5	GND	Ground
6	NC	No connect
7	I/O	Bidirectional data I/O
8	NC	No connect

3.1.1.4 Fingerprint sensor

The system is designed to support biometric authentication. Therefore, a fingerprint scanner is integrated onto the system. In the market, there are not plenty of sensors to buy and programme that are compatible with the controllers, so after researches the ZFM-20 series fingerprint identification module is chosen for the project which origins from China. During system construction, there occurred some limitations related to sensor. For instance, sensor datasheet cannot serve enough detailed information about the algorithm inside of it. The more technical vulnerabilities are explained in Chapter 4.

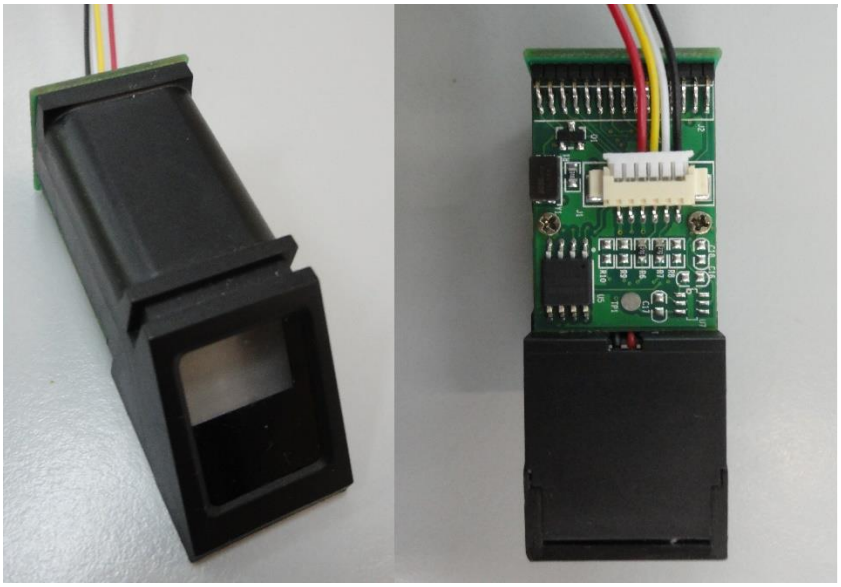

Figure 3.7 : Fingerprint sensor top view on the left, bottomside view on the right.

Fingerprint sensor in the system is used to take the raw fingerprint data in its image buffer. This sensor work with a DSP processor inside. All the basic processes are handled in the sensor side like image acquisition, feature extraction for fingerprint details, data conversion, and even compression. Table 3.5 illustrates the cable connections of the sensor. Pin number colours as cables on the Figure 3.7.

Table 3.5 : Fingerprint sensor cable connections [26].

Pin(Cable)	Name	Type	Function
1	Vcc	In	Supply voltage
2	TD	Out	Data output. TTL logical level
3	RD	In	Data input. TTL logical level
4	GND	Ground	Ground

Sensor scans the finger and it temporarily saves the finger image in the image buffer inside. The image format as shown in the Figure 3.8 is 256x288 pixels. It uses 4 bits of data, which is actually 16-bit gray level values. Moreover, there is fingerprint library, which is in flash memory where the data does not get affected when the power has gone. Therefore, data can permanently be stored in the sensor [26].

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	. . . .	$a_{1,286}$	$a_{1,287}$	$a_{1,288}$
$a_{2,1}$	.						$a_{2,288}$
$a_{3,1}$		.					$a_{3,288}$
. . . .			.	. . . .	.		. . . .
$a_{256,1}$	$a_{256,2}$	$a_{256,3}$	$a_{256,4}$	. . . .	$a_{256,286}$	$a_{256,287}$	$a_{256,288}$

Figure 3.8 : 256x288 pixels raw fingerprint image format in matrix illustration.

Communication protocol of the fingerprint sensor is crucial. During the design of system structure, creating packages, sending them to sensor and receiving the reply from that sensor are some operations that are handled via controller. Therefore, the standart data package format is needed to be known as in Figure 3.9.

Header	Module Address	Package Identifier	Package Length	Package Content	Checksum
2 bytes	4 bytes	1 byte	2 bytes	-	2 bytes

Figure 3.9 : Fingerprint sensor data package format.

Even it is enquired the transformation details of fingerprint raw data to characteristic file from the vendor, there was no return, so that transformed data is obtained from the sensor and used directly.

In the image buffer, there is the raw data of the scanned finger image. To get this data, it is needed to use indicated communication protocol format. Using the standart format and related instruction code, controller sends the package and wait for the acknowledge. Confirmation must be 00 and if it is, then via serial communication, sensor sends the raw data. The rest of the confirmation codes of the fingerprint sensor are given in the Appendix A. Fingerprint sensor has 56700 built-in baud rate that is possible to be changed by sending communication packages to the sensor from the controller.

In the market, there is not too many fingerprint sensors to be used for application purposes, but the one similar to in this study can also be found in [27].

3.1.1.5 RFID/NFC module

NFC, Near Field Communication, is an up-to-date technology that is even placed on our mobile phones. There are two basic communication types of it, one is Passive Communication and the other is Active Communication. In this thesis, not NFC but RFID aspect of the module is used.

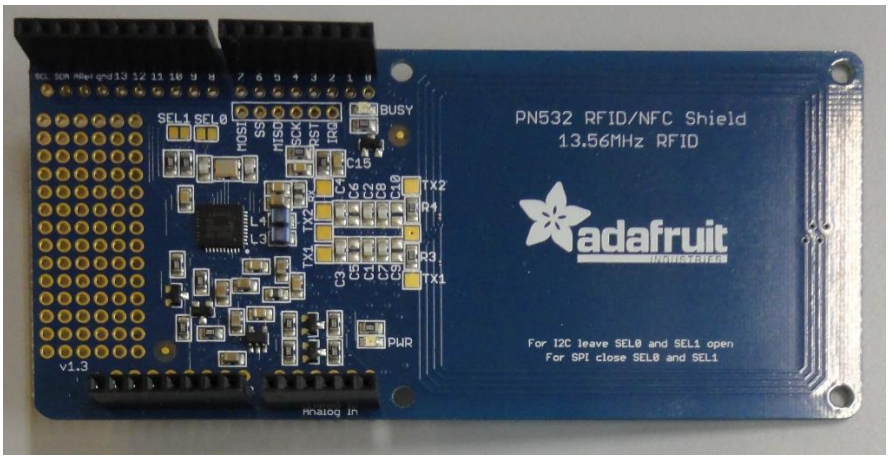

Figure 3.10 : RFID/NFC Reader/Writer module for admin node of the system.

This module as shown in Figure 3.10 is used in the admin part of the system. The question can occur related to why not smart card but RFID. This is because the project applicability is aimed to be increased by applying proposed algorithm not only smart cards but also contactless cards. RFID cards are more sensitive to cryptological attacks because of remote sensing approach from several centimeters; therefore, more reliable

algorithms are expected. This device is integrated on to the Arduino UNO in the admin side.

3.1.1.6 XBee modules

Wireless sensor network is trending technology that can be used in system communications. XBee sensors are the ones give possibility to create network. Even more, in IEEExplore, XBee is used mostly for biometric signal monitoring device as in the journals. XBee and its shield is given in Figure 3.11.

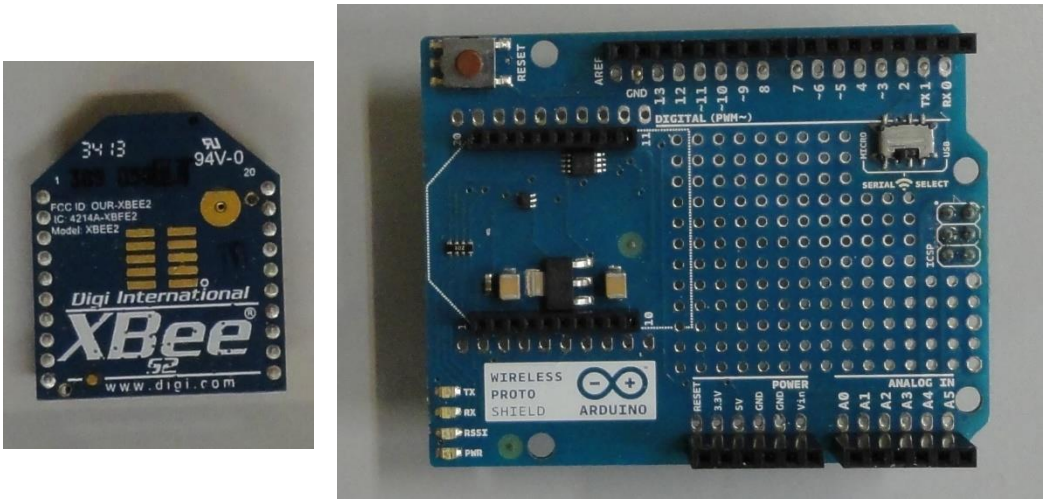

Figure 3.11 : XBee module and its shield.

XBee sensors have two types. If there is only one receiver and a transmitter, then the *series 1* type will satisfy the conditions. On the other hand, if there are much more nodes, in other words mesh network, *series 2* works well. This thesis proposes one node and one admin illustration in theory, but surely, it is forecasted that there are many access nodes to be controlled and even more than one admin for real life engineering applications. Therefore, *series 2* based module was chosen to be the system extended in the future. Unluckily, series 2 XBee modules are a little more complicated. To configure the XBee Radios, it is needed to use X-CTU software from vendor. Zigbee and XBee are not the same things. Zigbee is the name of the protocol such as 802, whereas XBee is the brand name of the module.

The chosen module, *XBee 2mW PCB Antenna - Series 2* has the following functions in Table 3.6.

Table 3.6 : XBee 2mW wireless antenna characteristics.

Specialities
120 meters range
Built-in antenna
2mW output
3.3V, 40mA
250 kbps maximum data rate

Connection between XBee devices is possible as star, mesh, cluster, tree and the pair. Because the proposed scheme has one access node and the admin, the XBees in the system will be set as one-to-one communication type.

Table 3.7 : XBee ATI commands for destination side.

Commands to program XBee sensor
+++
ATID 2001
ATIDH 0013A300
ATDL 40BD2B2C
ATWR

Figure 3.12 : XBee module coordinator/router indicator numbers.

XBee modules have some mode of operation. One is command mode to programme the module itself by using the commands in Table 3.7. For programming issues, each of the node with XBee must be indicated as router or coordinator. Each network can only and at least have one coordinator and several routers, or in some cases, some end devices. In our system as there are two XBee modules, one assigned as coordinator (admin node), and the other assigned as router (access node). This is handled by using special numbers behind of the XBee module itself, as Figure 3.12 shows them with red and green rectangles. Programming the XBee module itself is needed to have ATI

commands by using an USB apparatus with XBee on it inserted into the PC. In Figure 3.13, the shield switch is shown for USB communication regulation.

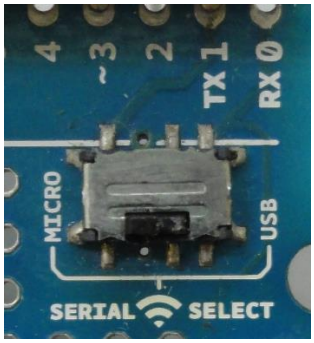

Figure 3.13 : XBee shield module switch.

3.1.1.7 Display

Screen is one of the most crucial elements in the system. New technologies support touchable screens, so they are not only output device but also an input device.

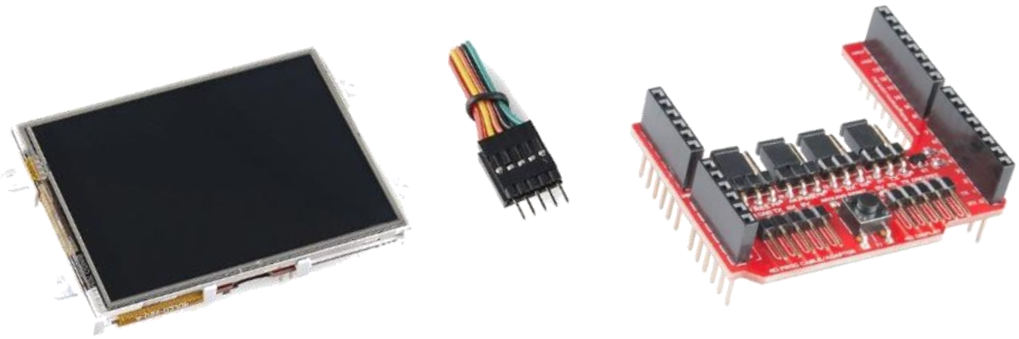

Figure 3.14 : XBee module, ribbon cable and its shield.

In this thesis, 4D Systems 32 PTU-AR is used as in Figure 3.14. This touchable display has the shield like some other modules in the system which saves designer from having to use wires on the Arduino. Shield of revision 2 serves loads of advantages like the flexibility of pin connections. Because it is used with some other shields like XBee and some sensors such as fingerprint, there can occur pin overlaps and power drawbacks. Putting delay at the very beginning of the code for display as 3500 ms is very crucial.

3.1.1.8 Serial ports

In the microcontroller of the system, there are several serial ports to be used for communication purposes. For the synchronization issues, there cannot be any I/O device that uses the same port. Therefore, multi port supported controller is better to be chosen. This thesis is also aimed to be a kind of guide for upcoming researchers who are going to develop applications on the related areas. Therefore, design details are shared from A to Z.

Table 3.8 and Table 3.8 illustrate the serial ports distribution of microcontrollers for I/O devices.

Table 3.8 : Controller serial ports in use for access node.

Serial Port	Serial Comm. Type	Device
Serial 0	Hardware Serial	USB conn.
Serial 1	Hardware Serial	Display
Serial 2	Hardware Serial	XBee sensor
Serial 3	Hardware Serial	Free to be used
Digital Pins (10, 11)	Software Serial	Fingerprint sensor

Table 3.9 : Controller serial ports in use for admin node.

Serial Port	Serial Comm. Type	Device
Serial 0	Hardware Serial	USB conn.
Digital Pins (12, 13)	Software Serial	XBee sensor

XBee sensor on the both sides use serial communication. This helps the designer to use *Serial.print()* command to create the communication between admin node or other devices.

Arduino has the ability to allow these serial ports, both software and hardware serial ones, synchronously communicate with controller at the same time. On the other hand, the scenario of proposed system must obey a synchronization algorithm. Figure 3.15 and Table 3.10 present all possible serial communication between devices.

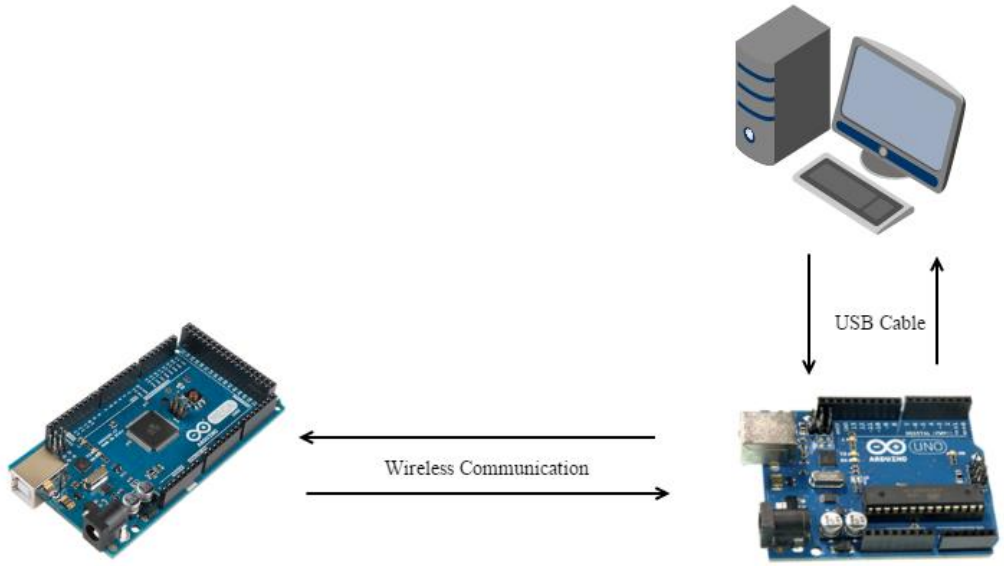

Figure 3.15 : Wired & wireless communications between devices of the system.

Table 3.10 : In-between communication list of the system.

Communication among devices
PC-to-UNO
UNO-to-PC
MEGA-to-UNO
UNO-to-MEGA

3.1.2 Construction steps

In this part, it is explained the way of integrating some electronic I/O devices to work all together. Before the scientific algorithms to be applied, the system is basically constructed. *Basically* word literally includes some basic functional tasks to be implemented like printing on the LCD touchable display, reading & writing some dummy data on the smart card, fingerprint scanning, wireless module communications etc. Whoever reads this thesis work, can easily understand the procedures for integration of some kind of sensors to be programmed independently at the first glance. After, combination of each goes until the last construction. Following sections are the steps of the construction that help the reader of this thesis work to reconstruct the same system for next academic purposes or just in mind. The whole proposed system is shown in Figure 3.16.

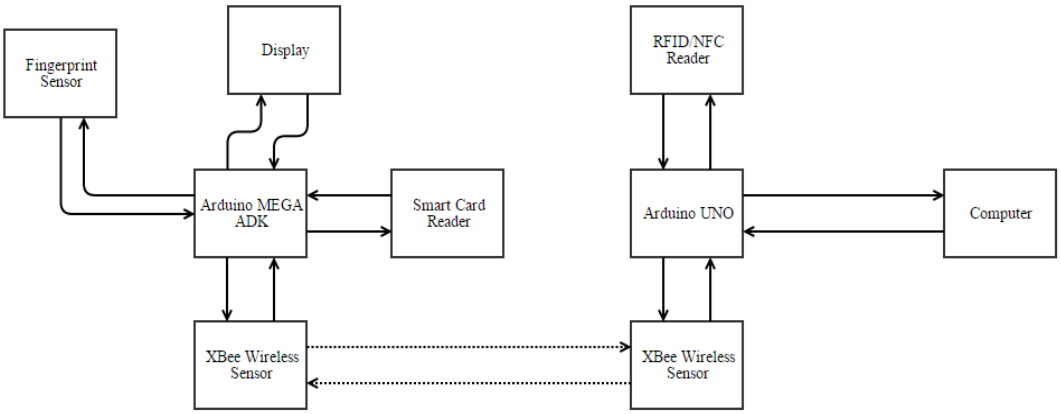

Figure 3.16 : The whole expected system.

3.1.2.1 XBee-XBee communication

In the system, XBee modules are included for wireless communication. After the configuration via programming in Section 3.1.1.6, they are ready for the communication test by using controllers. The first step is to place shield onto the controller, and XBee on the shield, too. There are two controllers as mentioned one for the admin and one for the access. They are going to communicate in wireless fashion as in Figure 3.17. Controllers have a built-in LED on them, so it should be used as indicator. In the controller side, one is sending a character as 'Y' and 1000 ms later 'S'. If the other wireless device reads 'Y', the related controller switches LED on, but if it is 'S', it switches LED off. This is a very basic and easy step to guarantee that controllers and wireless devices are working together. XBee sensors send data by using the serial communication.

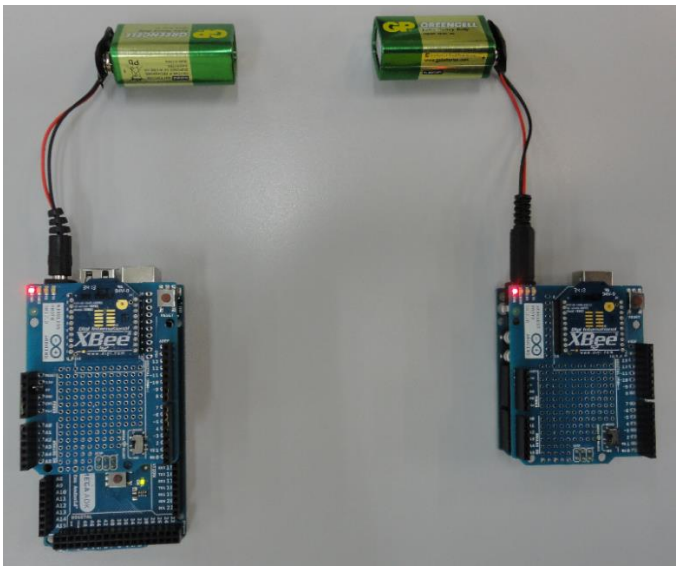

Figure 3.17 : XBee – Xbee communication.

On the other hand, the security issue must be resolved, even though it has a built in encryption. Whereas, by public key cryptography, there is to be a more secure implementation which this thesis defense.

3.1.2.2 Smart card read/write operation

After wireless communication is guaranteed, the smart card is needed to be integrated onto the system. Any dummy data can be written into the card and then readed. To do so, SmartCard class was constructed as the UML design includes. Read and Write functions can do the task by accessing the EEPROM of the smart card.

3.1.2.3 Fingerprint sensor alone

Fingerprint sensor is the most complex element in this system, so it is tested alone with a controller. All basic functions like scanning finger, converting and getting data into upper PC, storing finger template, authentication etc.

3.1.2.4 Fingerprint sensor – smart card reader together

As done the uploading template data to the upper PC successfully when fingerprint sensor alone, then the synchronization with smart card is expected. Finally, fingerprint sensor and smart card module are composed to work synchronously, too. User shows the finger, template is created and it is stored in the smart card. Even vice versa is valid; smart card data is read and fresh incoming fingerprint data is captured to be compared as in Figure 3.18.

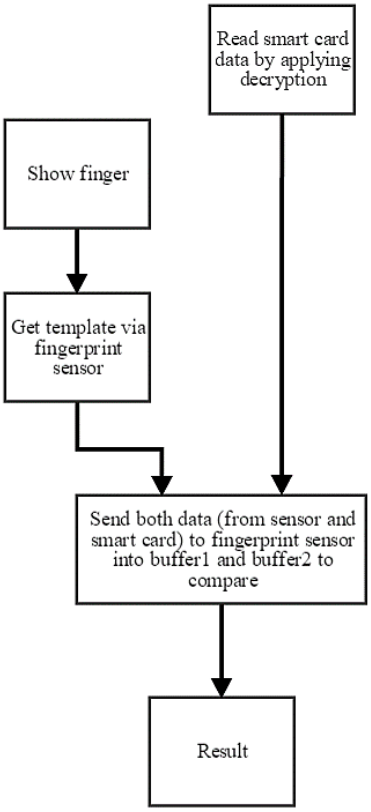

Figure 3.18 : Fingerprint sensor and smart card work together.

3.1.2.5 Display trials and integration

Close to the end of physical hardware contruction, only one controller and the only display together is to be concentrated on. First, the event handler functions for objects on the screen like buttons, keyboards, text box etc. (object list is given in Appendix B) are obtained, the reason why display is an input device, too. Then, display is integrated on the system as a last element.

Lastly, the whole system were constructed by including previously explained devices. Following Figure 3.19 illustrates the ACN related constructions physically with steps as the numbers indicate.

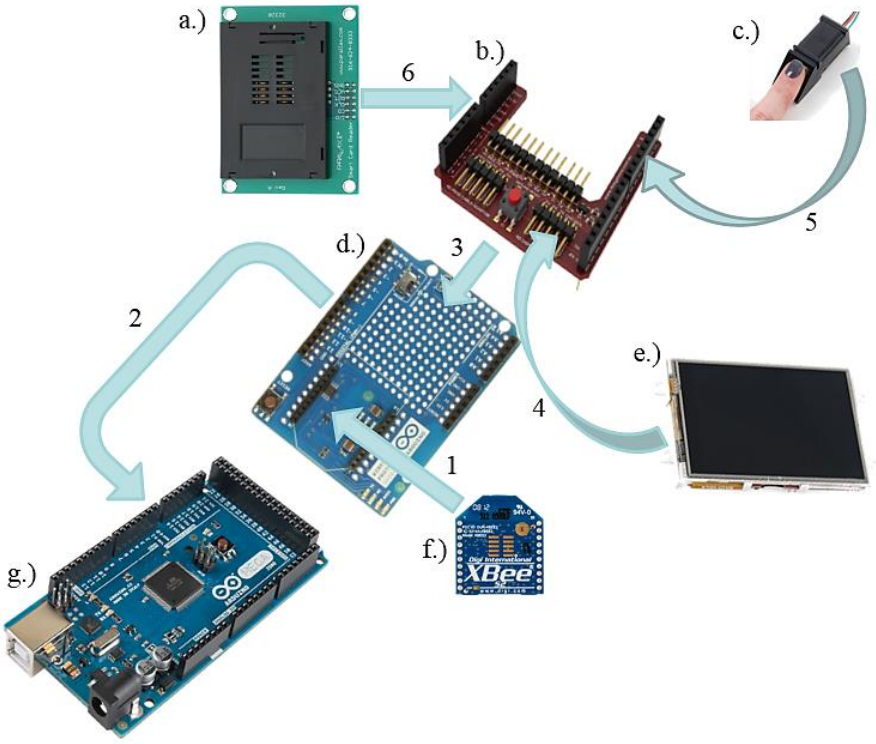

Figure 3.19 : Access node structure of the system together with connections.

3.1.2.6 Admin node construction

One of the two nodes, admin point of the system, provides monitoring for the supervisor. To do so, one another ‘access’ is needed, too. Previously registered admin had a PIN number and relatedly a NFC/RFID card. These types of cards distinguish from contact cards in terms of being contactless. In this study, the encrypted PIN number is stored in the card. For authentication purposes, it is demanded during ADN monitoring screen access. Figure 3.20 shows the physical structure of the admin hardware.

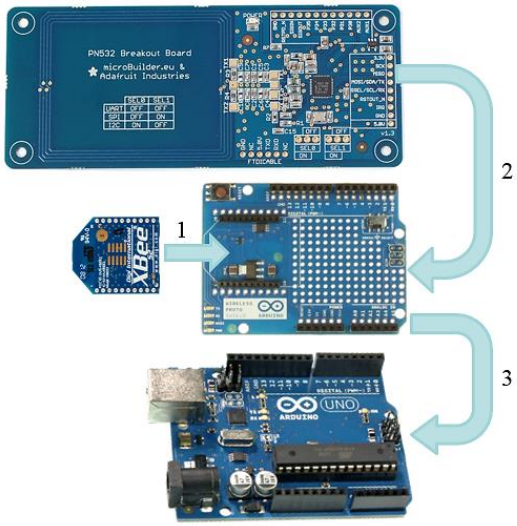

Figure 3.20 : Admin node structure of the system together with connections.

3.1.3 Communications Protocol

Synchronization and secure communication are the vital elements in this system design. As in the previous sections, each I/O device has its own communication protocol previously designed by the vendor, depending on the hardware. To run an efficient design, each element in this system was independently examined and all related communications protocol based libraries have been constructed and added into the main project path in the controllers' side. By the approach of object oriented programming, all libraries are 'called' in the main code playground of the controller. When it comes to completely constructed system, several devices require synchronization and wireless communication is open to be increased some steps upper in terms of security. To do so, own communications protocol which is application specific for proposed system is designed by obeying some scientific standards.

Bochmann and Sunshine indicates that protocol specifications can be divided into three basic branch as in the Figure 3.21. First, transition model, includes the *events* like commands, messages and timeouts. This model contains Petri nets and state machines. Another protocol specification is the programming language. By using a high-level programing language, a specific protocol can be handled as an algorithm. Lastly, the hybrid models compromise both the transition models and the programming language [28].

Petri nets are more prone to be mathematically implemented for future considerations by modelling the functional part of the system. It is a formal language with a graphical interface. On the other hand, implementing an algorithm to package and parse the package with one another algorithm –Diffie-Hellman–, especially very handy with a programming language, as the controllers understand. Therefore, these both approaches drove designer to hybrid models.

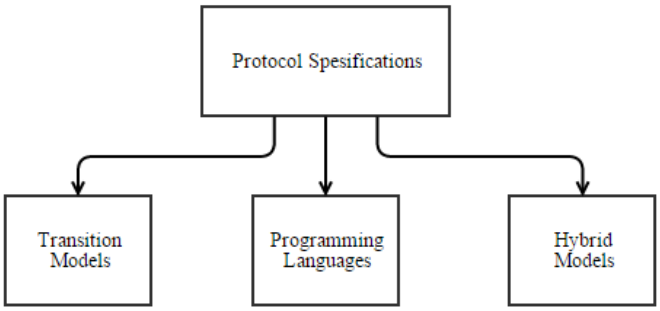

Figure 3.21 : Admin node structure of the system together with connections.

To conclude, in the design, the hybrid approach will be used to design the proposed approach first, and make programming after all, because C/C++ based microcontroller support programming environment. The aim is to obtain a neat approach.

3.1.4 Proposed protocol

As in communications protocols traditionally covered, it is not dealt in this thesis with-a-between layer based communication approach but the amongst different modules i.e. I/O devices and controllers. By using all of aforementioned hardware structure, synchronized, neat, robust and secure system is aimed with the specialized protocol during all operations. This could basically include serial communication issues which has already has its own protocol. However, in this work it is served a different idea that in the upper side of the serial protocol which is controlled by microcontroller software.

Abadi underlines that protocols that are designed must be understood in some other machines like access control. This will give a generic speciality to the design. Moreover, cryptography requires cost issue to be considered and if access control system is the case. There are two authentications type to be chosen: one way and mutual authentication [29].

Tablo 3.11 illustrates some terms that are used in pi calculus to define the cryptographic protocol in terms of math. But this is out of this thesis scope, presumably can be handled in future considerations.

Table 3.11 : Applied pi calculus grammar [30].

Grammar of the applied pi calculus for *processes*	
P,*Q*,*R* ::=	processes (or plain processes)
0	null process
P | *Q*	parallel composition
!*P*	replication
v n.*P*	name restriction
if *M* = *N* then *P* else *Q*	conditional
u(*x*).*P*	message input
ū‹*M*›.*P*	message output

The first step is to use a scientific design method to implement all the issues in the goal protocol design. Smart card and fingerprint related issues are needed to be taken into account. For security issues, non-invertible functions require a quite interest.

Exponentiation is not invertible, even more commutativity is valid which is advantageous for secret key establishment [31]. Commutativity is illustrated in Equation 6.

$$(g\,\hat{}\,x)\hat{}\,y \;=\; (g\,\hat{}\,y)\hat{}\,x \qquad \textbf{(6)}$$

This approach is crucial for thesis proposal for Diffie-Hellman algorithm, too. An attacker has an advantageous state to control power requirements of a smartcard [32]. There are some effective attacks related to power like Single Power Analysis Attack (SPA) and Differential Power Analysis Attack (DPA). Therefore, data stored in the smartcard should be in risk.

Specially, there are some specifically produced smart cards to handle some biometric data processing jobs even with security issues. These cards can handle biometric data comparion of two templates even inside of its own processor [33]. In this thesis, the smart card in the system, is not any special type, i.e. application specific, just for the regular one there is not any features about biometric data.

Match-off-cards are the ones to store biometric template of the cardholder and for each request, template travels from the card into the processor outside of the card. Match-

on-cards are specially handle matcing operation of stored template in the card and incoming one from outside with its built-in hardware structure [33]. This is the one in this thesis work, reason why security plays an important role.

All in all, the entire propects are to be considered during own communication packaging. The following Figure 3.22 is the proposed package format of the ACS in this thesis that has quite in common with any standart devices' communication protocol. However, synchronization is a very crucial point in multi modal sensory systems, the reason why headers of the package diverse and data complication is controlled.

Header	Address	Instruction	Data	EOP	*CRC
1 Byte	1 Byte	1 Bytes	Extendable	1 Byte	2 Bytes

Figure 3.22 : Proposed communication protocol package format, *CRC is optional.

Every single package that carry data has the header which is followed by address. Header and addess together define the source-destination pair. There can be 9 different address points for each node the reason why it is placed 1 byte for address part of the package. Following recalled Table 3.12 together with the header information is given for each pair.

Table 3.12 : In-between communication list of the system together with headers.

Communication among devices	Header of the pairs
PC-to-UNO	&
UNO-to-PC	?
MEGA-to-UNO	*
UNO-to-MEGA	!

Data can be any amount from source device to end device, so 'data' part of the package is extendable. On the other hand, this damages the readability of the package with the previously defined byte lengths. Then, the delimiter is used to control each part whether it goes into next part of the package or not.

Table 3.13 : List of possible values for package to be sent and received.

String	ASCII value	Assignment
*	42	Header (MEGA-to-UNO)
?	63	Header (UNO-to-PC)
!	33	Header (UNO-to-MEGA)
&	38	Header (PC-to-UNO)
1	49	Address / Instruction
2	50	Address / Instruction
3	51	Address / Instruction
4	52	Address / Instruction
5	53	Address / Instruction
6	54	Address / Instruction
7	55	Address / Instruction
8	56	Address / Instruction
9	57	Address / Instruction
.	46	EOP
|	124	Data delimiter

List of possible package format elements are introduced in Table 3.13. The reason why ASCII values are used is that the character values in terms of numbers are to be mathematically processed via cryptographic approaches.

Following Figure 3.23 is to illustrate a proposed case that access device sends Diffie-Hellman parameters at the very beginning of the key agreement, then data communication is driven. Details of the packaging, parsing for protocol together with Diffie-Hellman key exchange is presented systematically.

Algorithm: Pseudocode of the protocol with Diffie-Hellman Key Exchange

```
if access node is choosen and new access is demanded then
        1. calculate A from a, alfa, p for Diffie-Hellman process
        2. package = String(header) + String(address) + String(instruction code)
                + String(A) + delimiter + String(alfa) + delimiter + String(p) + delimiter + EOP
        3. Serial.print(package);
        4. while is acknowledge package for B key is not captured do
                listen the serial buffer
                if Serial.available == true then
                        for all data i=1:N in the buffer
                                incomingData += char(buffer[i])
                                delay
                        endfor
                endif
                Parse()
                        1. if incomingData[0]= expectedHeader then
                                2. if incomingData[1]= expectedAddress then
                                        3. if incomingData[2]= expectedInstructionCode then
                                                when it is for B, take B
                                                Serial.print Acknowledgement
                                                delay
                                                Extract rest of the package considering delimeter
                                        endif
                                endif
                        endif
          endwhile
        5. Encrypyt all outgoingData with the B parameter
        6. Serial.print outgoingData
        7. if any data comes then
                decrypt via B
                Parse incomingData
          endif
endif
```

Figure 3.23 : Pseudocode of the proposed protocol from ACN to ADN.

For future researches, some can be interested in the matmematical modelling of such protocols which is first drawn by petri nets as told formerly. Thanks to this, this thesis proposed protocol gets closer to hybrid model of the protocol design standarts. Figure 3.24 is the petri net model of this study.

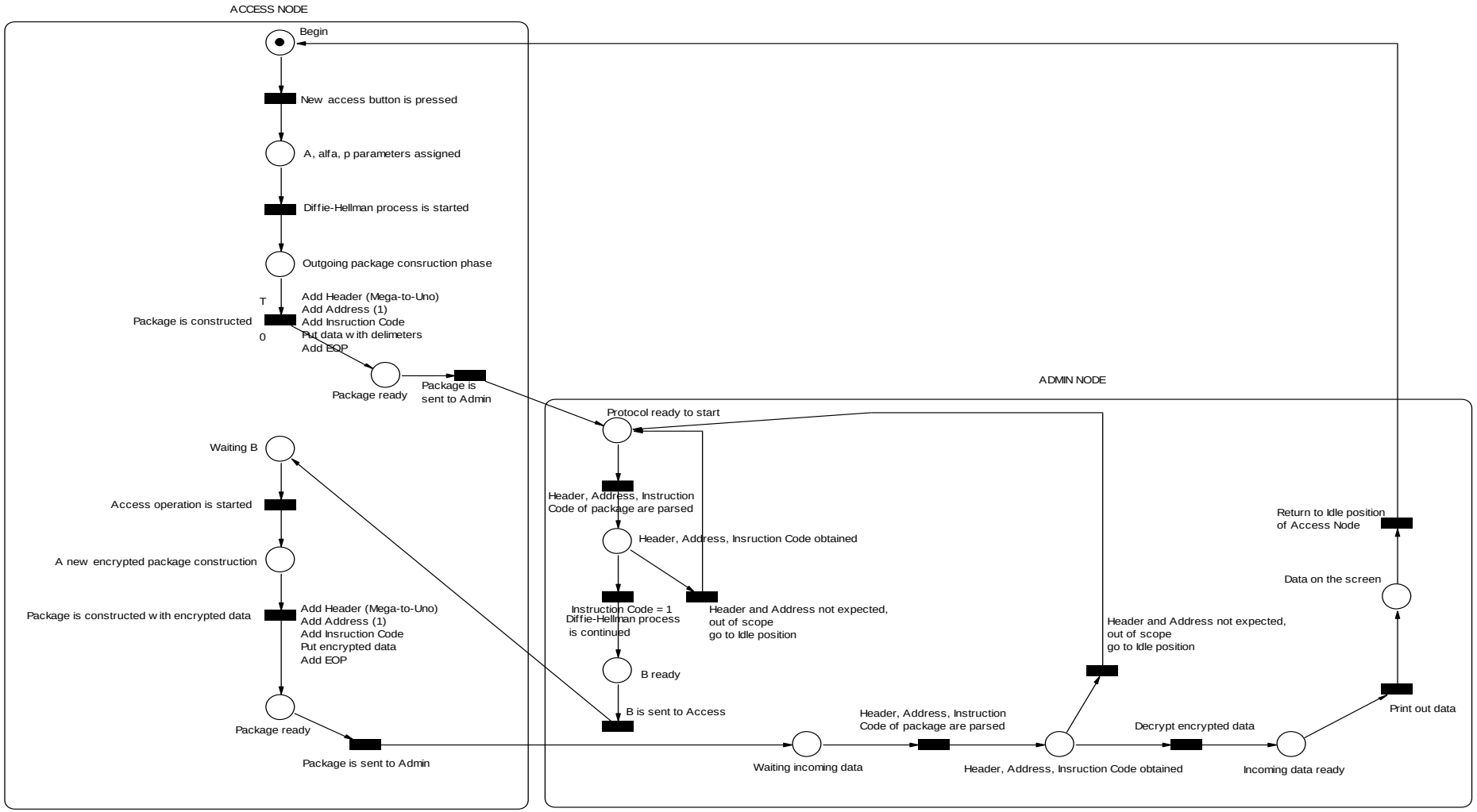

Figure 3.24 : Petri Net model of the proposed communication protocol.

3.2 Software Structure

Hardware part of the design has constructed the all physical layers of the system. After that, the control of the completely successful system level modelling projects requires visualized block & sequence diagrams. Eduardo B. Fernandez et al. claims that the crucial aspect of the access control pattern design is that the *"the rights assigned to roles"* [34], which is come up with an encapsulated solution for different users.

Software processes have several steps to be applied. In general, there are five stages needed to be considered: Analysis, Design, Implementation, Testing, and Maintenance. In this thesis, the first there is aim to be followed. Testing is also on the scope by applying some boundary cases, but the Maintanance is some other step is for industrial and commercial companies that support different from the academic approaches.

3.2.1 UML design of the system

Unified Modelling Language is the generic approach to software design projects which literally tells the designer about the details of the system structure. In bigger development projects, software construction starts with the UML diagram that satisfies the requirement analysis. This helps the designers to see further phases of the development and to understand each different modules of the projects that are obtained by different developers thanks to unified symbols. Moreover, in system engineering, relation of devices even in terms of hardware can be modeled by using the modelling language. By that way, the software issues related to the system would be handled more easily. In Figure 3.25, the designed system UML of this thesis is presented. There are sensor names as class demonstrations.

3.2.2 Pattern of the access control system

In software development projects, especially the object oriented ones; "pattern" is a neat approach to put your codes into the previously discovered programming style that helps to provide reusable solutions to common repeating problems. Torsten Priebe et al. claims that the security patterns are in the interest of system designers that releases some new patterns [35].

Torsten Priebe et al. indicates that like in classical pattern approach, in security system based patterns are described as in the structered form, too. More clearly, there are five elements in the structure to define a content of the pattern: intent, context, problem, solution, and consequence. *Intent* of the pattern basically tells the problem to be solved thanks to pattern. The *context* enlightens which fields to be applied by that pattern. Thirdly, the *problem* as on its name describes the problem together with the requirements to be applied of this pattern. *Solution* gives details of the problem solution via UML diagrams and lastly the *consequence* part indicates the implications of the pattern by its constraints [35]. In this thesis, the same approach is used, too, during the implementation of UML diagram the previously defined access control system related pattern is used together with the proposed software structure of the sensors. The proposed UML of the system is shown in Figure 3.25. *Role*, *Privilege*, and *Permission* classes are stand for RBAC which is a pattern in OOP designs gives different roles to different users [36] [37].

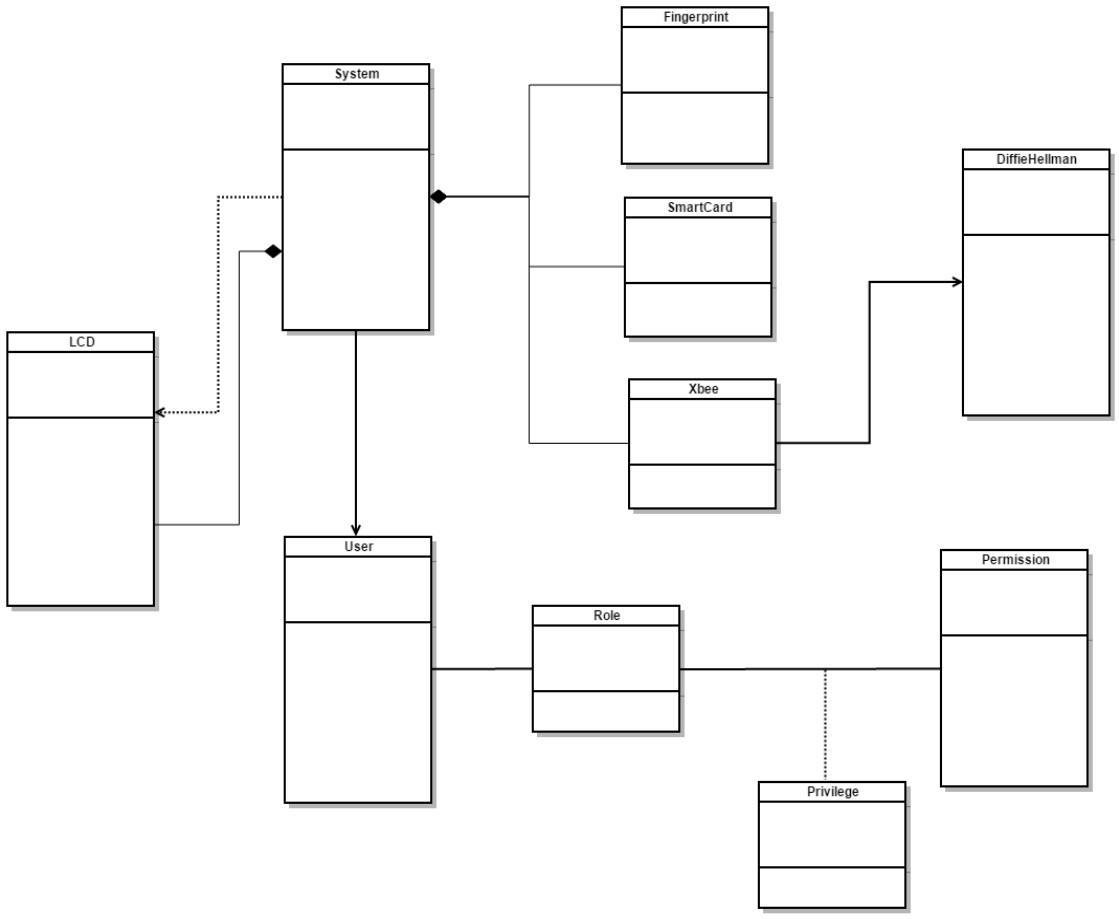

Figure 3.25 : UML design of the system with role based acces control pattern.

4. SYSTEM ANALYSIS

The designed system with proposed application based algorithms is needed to be revised and tested after the end of construction. During the tests, there can occurs some limitations that restrict the user. Even more, while the system is being constructed by an engineer, unexpected and unforecasted situations can occur. Therefore, after the design phase finished, it is better to present the analysis of the whole system related to thesis that illustrates the system details, limitations, extreme cases etc. As a result, the trouble shooting becomes easier to handle for whoever read and use this thesis.

4.1 Sequence Diagram of the System

The first step is to understand how system works in application manner. System steps can be modelled by using diagrams to understand them in details. Figure 4.1 shows how the system works during user access. This model is called *UML Sequence Diagram*. Actions can be presented in this diagram related to actors. In the access control, the user as the main actor communicates with the system. This is mostly is handled by the display that is not only output by also an input device. A related diagram in the literature is supplied in [38].

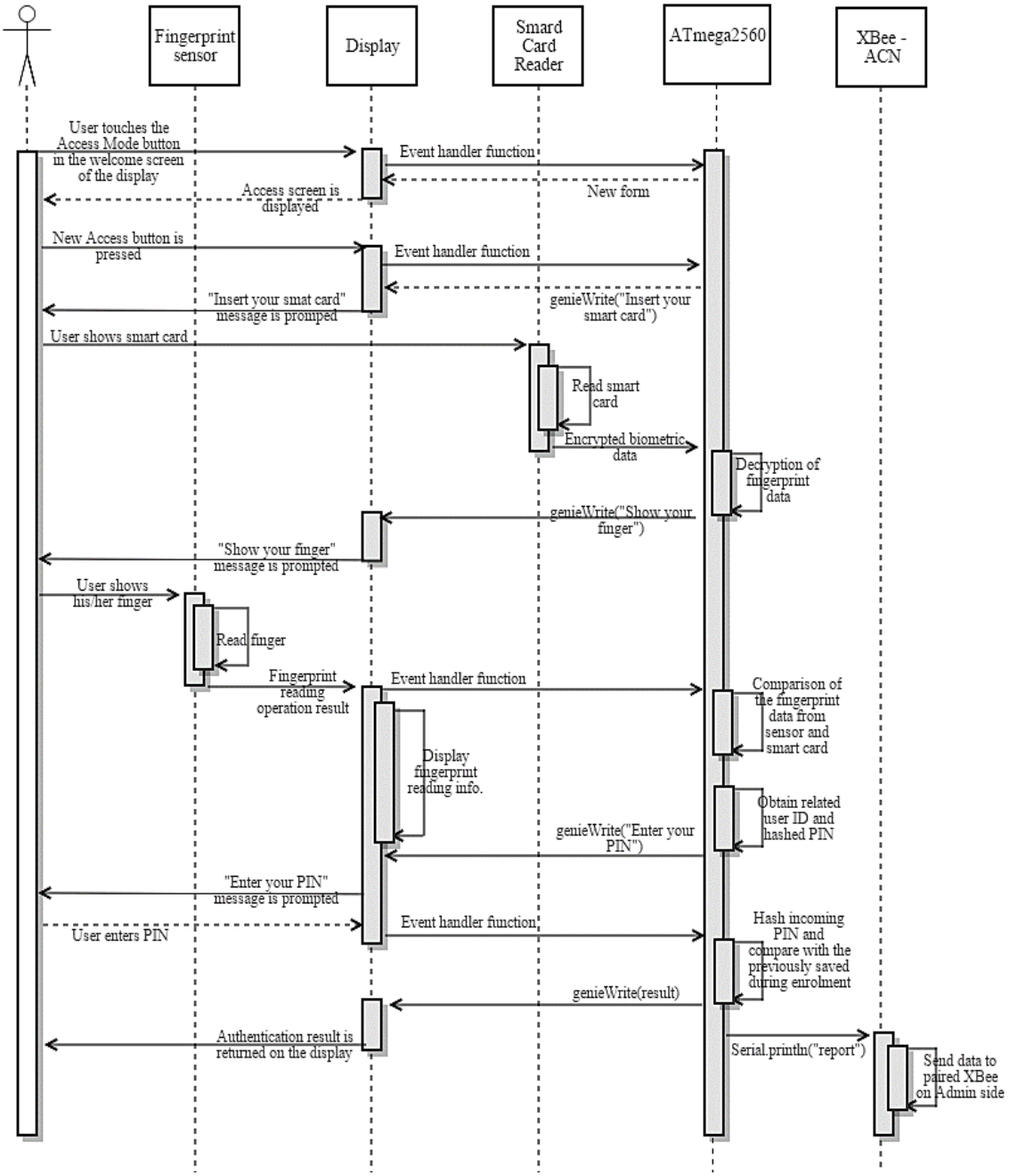

Figure 4.1 : UML sequence diagram of ACN.

4.2 Vulnerabilities and Limitations

Reading data from the fingerprint sensor by using Arduino controller has some limitations for raw image of the user which is 256x288 pixels. These values correspond approximately 72000 bytes that is 36000 actually, because every two adjacent pixel is sent as one byte. Even 36000 bytes are cannot be transferred to Arduino via serial communication without any loss in the baud value 57600 for fingerprint sensor. Taking 36000 byte data from the fingerprint sensor approximately require 20 seconds with 9600 Baud Rate. This is more than a lot, so making image processing in the raw finger image by controller occurred impossible. Furthermore, fingerprint sensor is such a black box in terms of image processing techniques. As Figure 4.2 emphasizes, fingerprint sensor does not gives details about the standarts of raw finger image conversion into template like which algorithms to apply, how to compare the whole database for each upcoming authentication finger etc. It is just possible to get transformed values illustrated as in Figure 4.3 same finger acquisition twice times.

Even the vendor and the supplier do not give detailed information related to hardware and algorithm. Therefore, there become prons the output of the sensor is not known very vell. The character stream from the sensor output is obtained. The image buffer 1 and image buffer 2 stand for the twice fingerprint scanning to be loaded the extracted char stream inside of them. Then, comparison is handled whether the both scan of the fingerprint owes at the same finger or not. If they match, the template is generated.

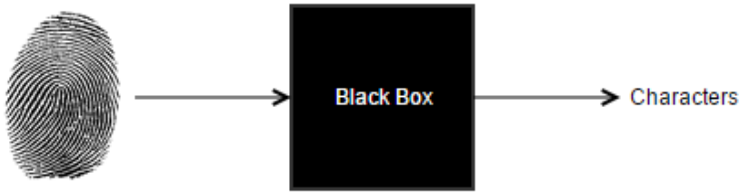

Figure 4.2 : Vulnerabilities related to fingerprint sensor.

[D A T A]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	EF	01	FF	FF	FF	FF	02	00	82	03	01	5B	1D	00	00	FF
1	FE	F9	FE	F0	06	C0	02	80	00	80	00	80	00	00	00	00
2	00	00	00	00	00	00	00	00	00	00	00	00	00	80	02	C0
3	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
4	00	4C	19	AB	1E	40	1B	81	7E	69	1E	A8	9E	24	21	9B
5	1E	52	22	6C	1E	0D	2D	5B	FE	48	B0	00	BE	75	B0	94
6	DE	70	38	6C	7E	67	C3	AC	5E	5E	8E	23	17	16	1C	85
7	3F	47	21	18	7F	30	AA	19	7F	2A	2D	41	7F	1C	37	82
8	FF	3D	BB	C1	BF	34	9F	02	3C	24	68	EF	01	FF	FF	FF
9	FF	02	00	82	46	C3	42	BC	4C	41	81	5D	51	10	1F	9B
A	2D	9E	DC	3B	37	8B	CA	B2	38	0E	A1	32	53	92	E4	78
B	61	2C	D5	98	3C	8B	C7	13	4D	92	DC	39	59	AD	6B	F6
C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

[D A T A]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	EF	01	FF	FF	FF	FF	02	00	82	03	01	52	20	00	00	FF
1	FE	E1	FE	C0	06	C0	02	80	00	00	00	00	00	00	00	00
2	00	00	00	00	00	00	00	00	00	00	00	00	00	80	00	C0
3	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
4	00	59	0E	5C	3E	53	A0	EA	DE	0E	A1	5E	7E	47	22	C1
5	7E	70	25	E8	7E	59	A9	EB	BE	0D	AA	05	9E	14	33	1B
6	DE	4F	B7	40	7E	65	15	E1	DF	4E	28	58	9F	2B	AA	1B
7	DF	38	31	19	5F	31	34	01	DF	23	3D	C3	5F	74	BE	2C
8	97	47	8E	56	FC	3C	26	02	7C	26	2B	EF	01	FF	FF	FF
9	FF	02	00	82	58	93	9D	7D	35	26	1C	1D	3A	15	62	9A
A	31	18	61	1B	3B	11	4C	58	47	12	45	B8	53	99	5C	D8
B	5B	19	A3	B8	68	34	15	F8	57	97	DF	99	61	34	6C	76
C	3F	11	C8	37	43	13	86	97	29	14	61	13	00	00	00	00
D	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Figure 4.3 : Comparison of the same fingerprint data at different times.

Characters in Figure 4.3 are the examples of the same finger's post-processed data. In this thesis, it is tried to understand the relation between these characteristic values of a fingerprint that are captured in different times like one is during enrolment for smart card and the other is during access operation from the freshly requesting user. The experiment on the thesis is to be first reading the card from the person and requesting the finger. In Figure 4.3, every red colored values are the communication package related ones.

There are several metrics to be extracted from the fingerprint output data. First, all smart card and live fingerprint characteristic data can be compared with respect to similarity such as Pearson Correlation, similarity weights etc. but the other limitation is that the Arduino control card is lack of data storage and parameter lengths. Therefore, summing operation can exceed the buffer size which does not allow to use some data mining approaches as mentioned, and so just the basic comparisons like Euclidean distance control handled.

4.3 GUI

Admin and the access nodes are in use by at least a user even admin or entrant who expects to have a visual monitoring interface both for input and for output. Therefore, there are some designs for proposed system to make it easier to construct a link between user and the system. For colorful designs that appeal users, there are some sources on the internet that designer can download and use free for non-commercial projects. To do so, 'icon' key word can be searched on the search engines. Visual C# allows the designers to upload some images in to elements on the forms.

Following sections visually illustrate the access node and admin node related GUI designs on the scope of thesis for touchable display and desktop application respectively.

4.3.1 User access node touchable LCD GUI

User who uses access part of the system comes across the resistive touch LCD. Therefore, LCD screen is used as the input device, too.

At first, there is a welcome screen to direct user to *Enrolment* for new user registration, or *Access Application* as the main part of the system. Figure 4.4, 4.5 and 4.6 show three main forms of the interface.

In the welcoming or in other words idle screen, user can select one of two choices: *Enroll* or *Access Mode*. In Enroll mode, a new user can register, while in the Access Mode the control of access is started.

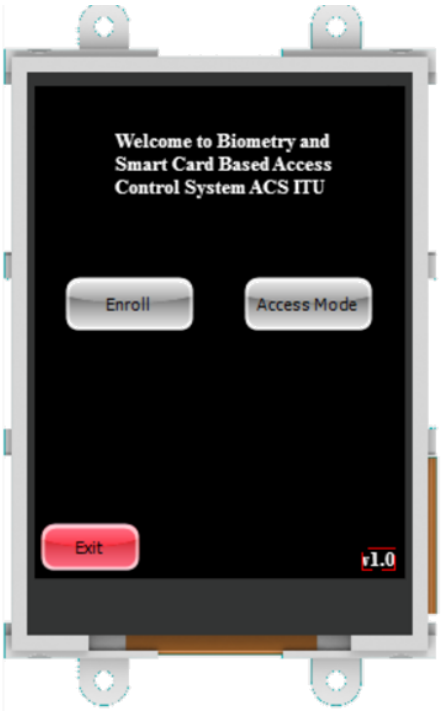

Figure 4.4 : Welcome screen of the ACN.

In Figure 4.5, new enrolment screen is presented. Here on this form, user can enter requested information bu using QWERTY keyboard. On spot, access mode can be started or new user can exit. All data is volatile until the ‘saved’ message is promted.

Figure 4.5 : New enrolment screen of the ACN.

Finally yet importantly, access screen can be reached for new access. By pressing the NEW ACCESS button, all sensors get prepared. In system response box, the guides for the user are shown.

Figure 4.6 : Access screen of the ACN.

4.3.2 Admin panel ACS monitoring GUI

Admin part of the system, both for the hardware and the end user interface is depended on the Windows running PC. Therefore, the monitoring desktop application is constructed on the Visual Studio 2010 C# development platform as the Windows form application. The application itself is designed visually for end user as much friendly as possible. Figure 4.7 and 4.8 show the entrance and monitoring screens respectively.

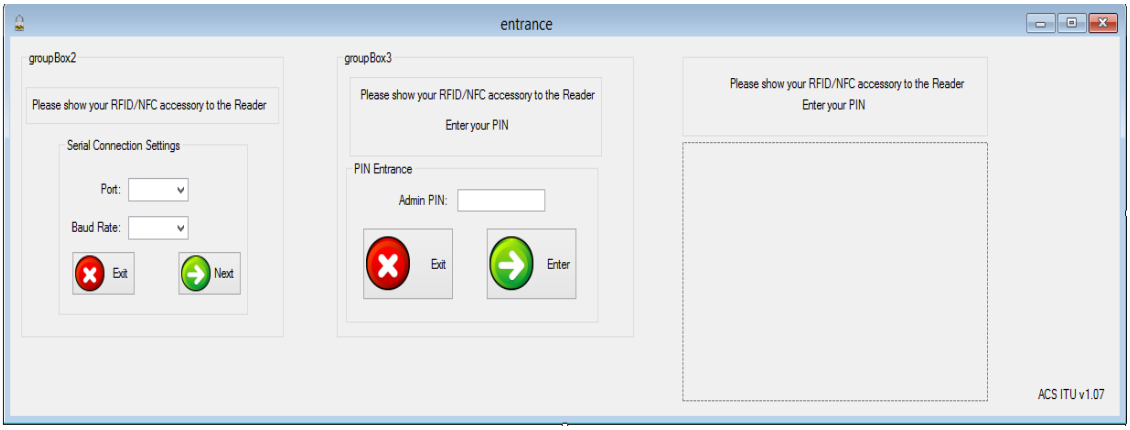

Figure 4.7 : Admin entrance screen of the ADN.

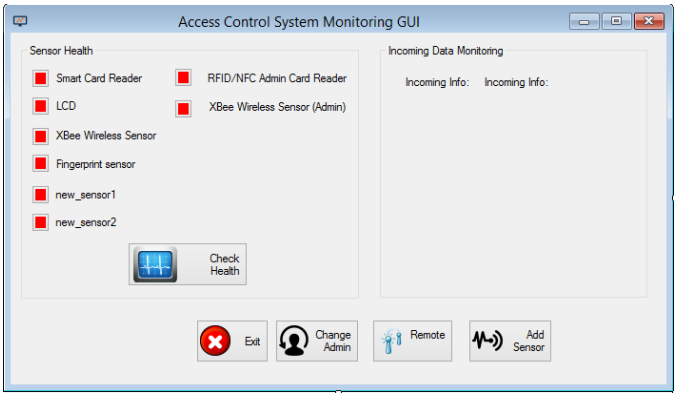

Figure 4.8 : Monitoring screen of the ADN.

In Figure 4.8 some buttons like change admin, check sensor health, add sensor etc. is for future considerations and has dummy code inside for now; in the manner of application engineering can be filled them up.

4.4 Overall Analysis

Fingerprint sensor has some details about biometric metrics as introduced in the Chapter 2; False Acceptance Rate-FAR <0.001% and False Reject Rate-FRR <1.0%.

Moreover, execution i.e. authentication certainity and execution time are needed to be analyzed. Fingerprint sensor is tested for the certainity and execution time at the end of the design for performance issues. Then, Table 4.1 and Table 4.2 were obtained.

Table 4.1 : Fingerprint sensor certainity percentages.

Person	Precision of the fingerprint data
A	%81
B	%69
C	%72
D	%60
E	%78

Table 4.2 : Fingerprint sensor authentication execution time.

Person	Time (ms)
A	1170ms
B	1207ms
C	1163ms
D	1126ms
E	1141ms

Furthermore, the analysis of two same-like fingerprint data one from previously stored smart card and the other from live data comes from sensor as in Figure 4.9 is illustrated. During enrolment user shows biometric data that goes into the card which is not stored by remote server due to gain user's reliance.

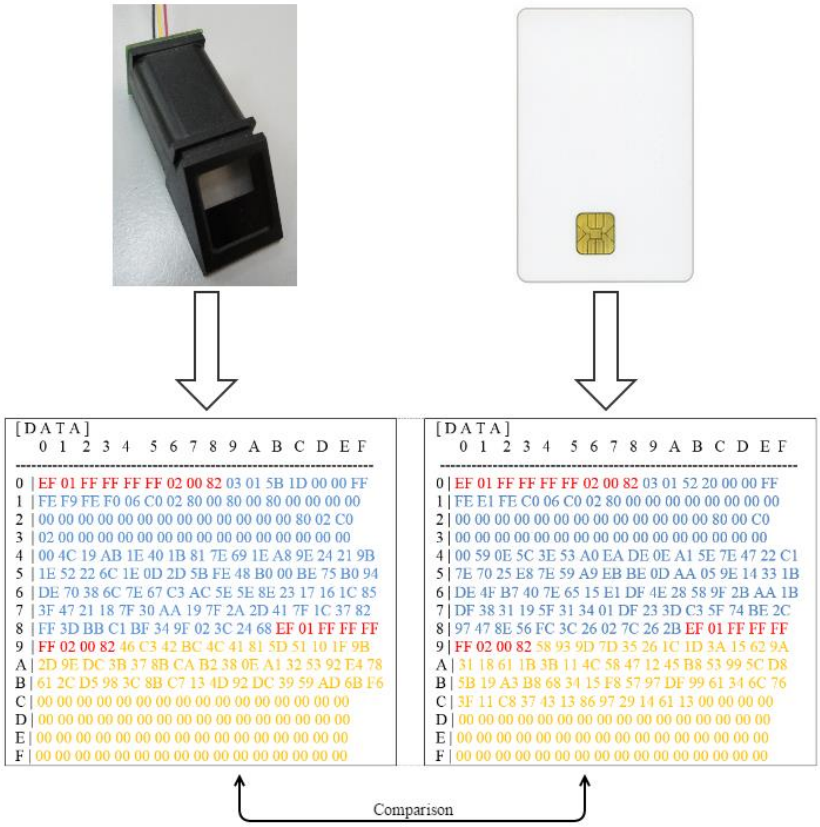

Figure 4.9 : Comparing two data of same fingerprint.

In Figure 4.10, the processed raw fingerprint data is analyzed by Euclidean Distance as in equation 7. The tilt dependent fingerprint data is taken into consideration which is another limitation, too. On the case, both enrolled data and access data are meet in terms of fingerprint position on the sensor, their relation is analyzed.

$$distance(a,b) = \sqrt{\sum_{n=1}^{k}(a_n - b_n)^2} \qquad \textbf{(7)}$$

There can occur some questions like why not some other correlation methods such a Pearson Correlation together with similarity calculation. It was tried during thesis but due to the performance issues in the 8-bit controller, they did not work well.

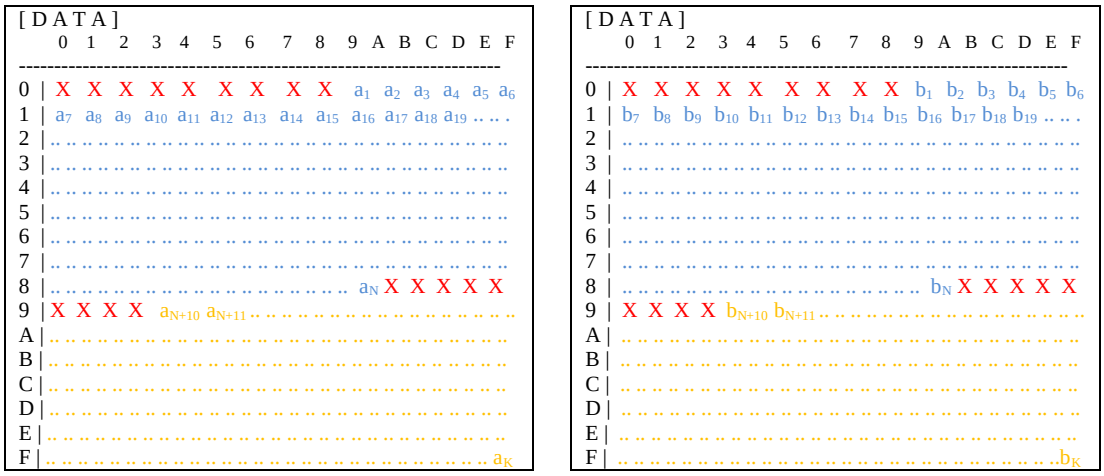

Figure 4.10 : Values to be processed in Euclidean distance.

During the calculation, each communication package values of fingerprint sensor in the finger data are skipped as shown with red X in Figure 4.10. All the rest with blue and orange coloured values are considered during the calculation of Equation 7.

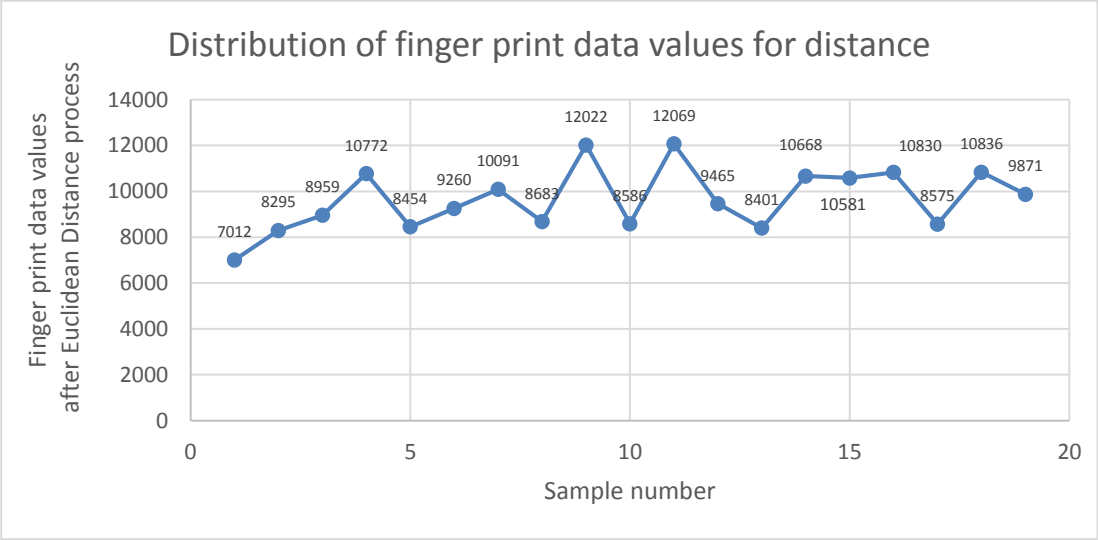

Figure 4.11 : Analysis of data from fingerprint sensor.

In Figure 4.11, the processed raw fingerprint data, in other words character file values are analysed by Euclidean Distance and analyses for each trial is drawn in total manner. Over much more 1000 sample from several people even at different times were analyzed, the lowest and highest values are recorded. No less than 6000 and much more than 13000 value is obtained. These values seem to be the limit for our decision algorithm. More importantly, for each user in the system is expected to show two times of his/her same finger. Then, these two values are operated for comparison as if smart

card originated data and live sensor data are checked against. Euclidean distance is the one parameter to decide whether data in the smart card and the data of user who demands to access system is same or not. The other parameter stems from the Equation 4. The twice times fingerprint data scanning is also used to calculate a unique number just after the comparison for Euclidean Distance. The difference between two data samples are considered as flexible error, ε, which is then can be used during authentication.

All the controls above are the additional checks after the fingerprint sensor control inside. First, it does control the smart card data with its own value in flash memory, then, our additional checks are applied for more strength.

5. CONCLUSION AND FUTURE CONSIDERATIONS

Secure, scientifically covered general purpose access control system was designed. Biometric information of human, i.e. fingerprint, was safely captured and processed. As proposed, trending development kits, Arduinos, were used to be in part of an scientific approach with their low memories which is a considerable problem for algorithms and complexity area. Smart card with low memory and without extra security feature inside is successfully integrated on the system. The GUI issue of the system, both for the administrative approach and for the arbitrary user on the access node was successfully designed.

Future technologies are seem to bring the wearable gadgets into daily usage. Some watches, biometric sensors, etc. are worn and technologically well-equipped to monitor some specific tasks. If it comes the proposed general purpose access control system, it is forecasted that the system is open to be worked for wearable technology support that is even decorated by NFC technology, then it is so easy to wear any NFC supported device and be an element of the system.

This work could be addressed to payment systems which have the standards EMV to be satisfied for further industrial approaches. The number of biometric sensors can be increased and by that way multi-modal approach strengthens. With XBee series 2, system is considered to be extended into mesh structure with more nodes of access and admins. Android based control can be added to system thanks to Arduino MEGA ADK, where ADK abbreviates the Android Development Kit together with its USB port.

No security applied for wired connections/communications, this can be extended. OpenCV related EMGUCV libraries were added into the system for following image processing applications for admin node. Multi language for GUI both for the admin and for the access node can be added. Logging information can be stored in a DBMS.

Additionally, admin's face can be added up into the authentication process to be stored as a template in the RFID card. By that way, multi modal approach will be supported, too. The case is shown in Figure 5.1.

To conclude, system level modelling from hardware to software details were successfully completed in the scope of academic approaches and hypothesis was achieved.

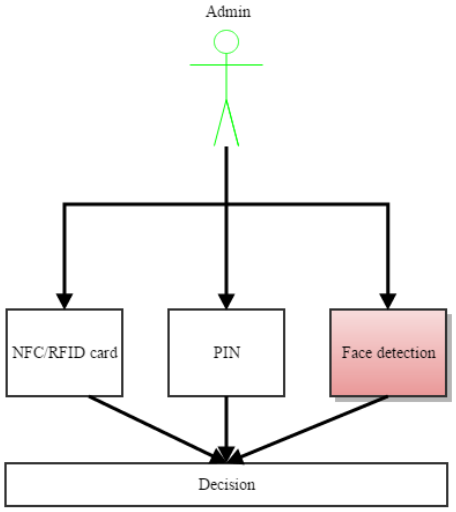

Figure 5.1 : Future work for the admin node.

Finally, it is better to present last version of the whole system that works successfully. In Figure 5.2, it can be seen the system including both the access part on the left side and the admin part on the right side operate. Also, there is the admin PC which monitors the accesses via secure wireless communication on the graphical user interface.

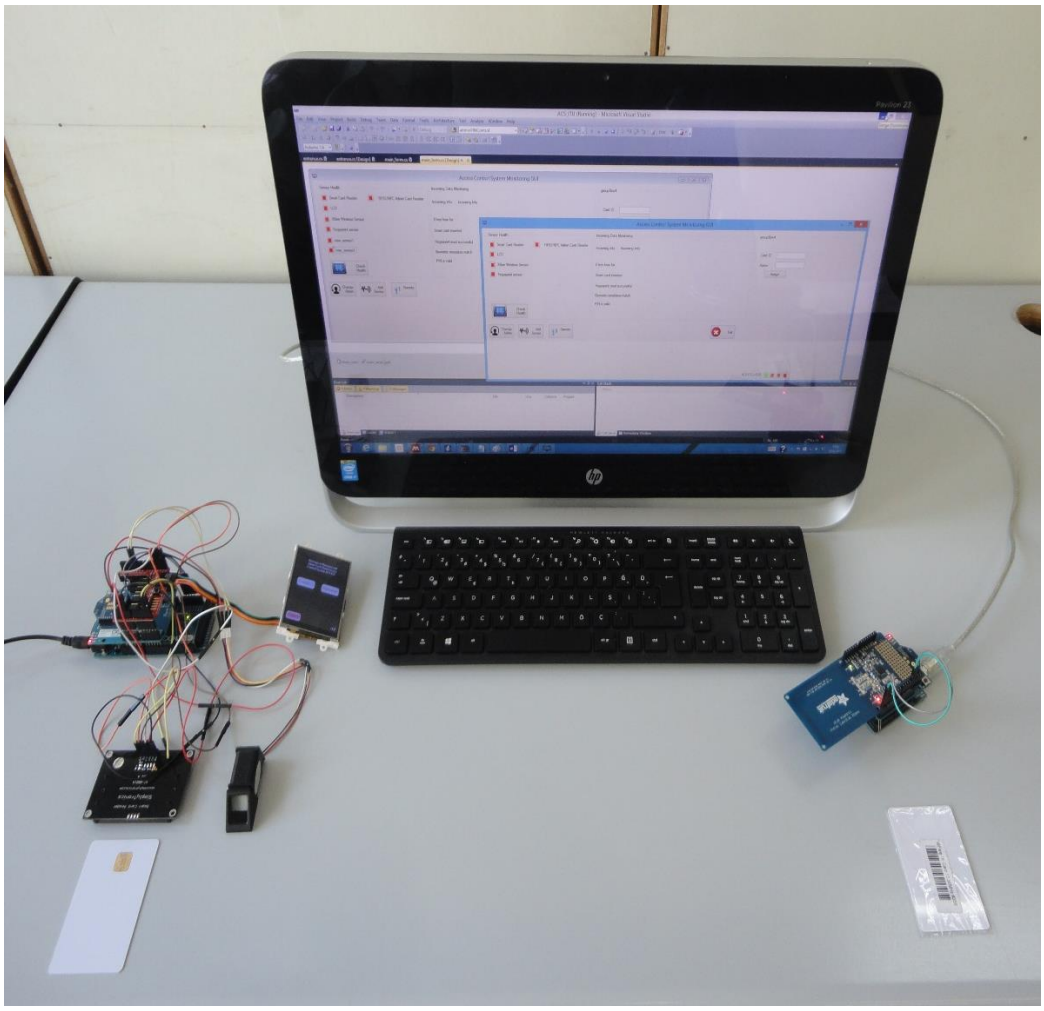

Figure 5.2 : Last version of the successfully working constructed system.

REFERENCES

[1] **Driscoll, E. C., Ph, D. & Fowler, R. C.** (1989). A Comparison of Centralized Versus Distributed Architectures in Biometric Access Control Systems. Security Technology, 1989. Proceedings. 1989 International Carnahan Conference, 193–198.

[2] **Sunehra, D.** (2014). Fingerprint Based Biometric ATM Authentication System. International Journal of Engineering Inventions, June 2014, vol. 3, pp. 22–28.

[3] **Harrison, B., Consolvo, S. & Choudhury, T.** (2010). Using multi-modal sensing for human activity modeling in the real world. Handbook of Ambient Intelligence and Smart Environments. 1–24.

[4] **Abdullah, M. a M., Al-Dulaimi, F. H. a, Al-Nuaimy, W. & Al-Ataby, A.** (2011). Smart card with iris recognition for high security access environment. 2011 1st Middle East Conf. Biomed. Eng. MECBME, 2011, pp. 382–385.

[5] **Chen, Y. & Yeh, L.** (2005). An Efficient Authentication and Access Control Scheme Using Smart Cards. 11th Int. Conf. Parallel Distrib. Syst. 2, 78–82.

[6] **Kumar, P., Indrani, B. & Amuthaprabakar, M.** (2014). An Efficient Password Based Authentication Scheme Using Time Hash Function and Smart Card. International Journal of Emerging Technology and Advanced Engineering, vol. 4, issue 6, June 2014.

[7] **Hai-Jian, F., Cheng-Wei, C. & Chang-Wei, Z.** (2011). Research on application of Ethernet-based fingerprint identification system in college laboratory management. Proc. - 2011 4th Int. Symp. Knowl. Acquis. Model. KAM 2011 274–276.

[8] **Tulyakov, S., Farooq, F., Mansukhani, P. & Govindaraju, V.** (2007). Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognit. Lett. 28, 2427–2436.

[9] **Nandakumar, K. & Jain, A. K.** (2008). Multibiometric template security using fuzzy vault. Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference pp. 1-6.

[10] **Jain, A. K., Ross, A. & Uludag, U.** (2002). Biometric Template Security : Challenges and Solutions. Secur. Watermarking Multimed. 4675, 629–640.

[11] **Al-Haija, Q. A., Tarayrah, M. Al, Al-Qadeeb, H. & Al-Lwaimi, A.** (2014). A Tiny RSA Cryptosystem based on Arduino Microcontroller Useful for Small Scale Networks. Procedia Comput. Sci. 34, 639–646.

[12] **Soyjaudah, K. M. S., Ramsawock, G. & Khodabacchus, M. Y.** (2013). Cloud computing authentication using cancellable biometrics. IEEE AFRICON Conf.

[13] **Banirostam, H., Shamsinezhad, E. & Banirostam, T.** (2013). Functional control of users by biometric behavior features in cloud computing. Proc. - Int. Conf. Intell. Syst. Model. Simulation, ISMS 94–98.

[14] **Uludag, U., Pankanti, S., Prabhakar, S. & Jain, A. K.** (2004). Biometric cryptosystems: Issues and challenges. Proc. IEEE 92, 948–959.

[15] **Onyesolu, M. O.** (2012). ATM Security Using Fingerprint Biometric Identifer : An Investigative Study. 3, 68–72.

[16] **Zhu, H.-H., He, Q.-H., Tang, H. & Cao, W.-H.** (2011). Voiceprint-biometric template design and authentication based on cloud computing security. Int. Conf. Cloud Serv. Comput. 302–308.

[17]http://en.wikipedia.org/wiki/Biometrics, Date retrieved: March 2015

[18] **Jain, A. K., Hong, L. & Kulkarni, Y. A** (1999). Multimodal Biometric System Using Fingerprint, Face, and Speech. International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA) 182–187.

[19] **Yang, J. C.** (2010). Biometrics verification techniques combing with digital signature for multimodal biometrics payment system. Proc. - 2010 Int. Conf. Manag. e-Commerce e-Government, ICMeCG 2010 405–410.

[20]https://books.google.com.tr/books?id=aXz0BwAAQBAJ& , Date retrieved: March 2015

[21] **Diffie, W. & Hellman, M. E.** (1976).New Directions in Cryptography Invited Paper. IEEE Trans. Inf. Theory 22, 644–654.

[22]http://tr.wikipedia.org/wiki/Diffie–Hellman_anahta , Date retrieved: March 2015

[23]http://www.arduino.cc/en/Main/ArduinoBoardMegaADK?from=Main.ArduinoBoardAD , Date retrieved: April 2015

[24]https://www.arduino.cc/en/Main/arduinoBoardUno , Date retrieved: March 2015

[25]https://www.parallax.com/sites/default/files/downloads/32320-Smart-Card-Reader-v1.0.pdf Date retrieved: March 2015

[26]http://www.adafruit.com/datasheets/ZFM%20user%20manualV15.pdf Date retrieved: March 2015

[27] Pro, F. SM630 Fingerprint Verification Module User Manual. 1–25 (2008).

[28] **Bochmann, G. & Sunshine, C.** (1980). Formal Methods in Communication Protocol Design. IEEE Trans. Commun. 28, 624–631.

[29] **Abadi, M.** (2007). Security Protocols : Principles and Calculi Tutorial Notes. Foundations of Security Analysis and Design IV Lecture Notes in Computer Science Volume 4677, 2007, pp. 1-23.

[30] **Ryan, M. D. & Smyth, B.** (2011). Applied pi calculus. Cryptology and Information Security Series, vol. 5, chap. Applied pi calculus, pp. 112–142.

[31] **Abadi, M., Blanchet, B. & Fournet, C.** (2007). Just fast keying in the pi calculus. ACM Trans. Inf. Syst. Secur. 10.

[32] **Batina, L., Örs, S. B., Preneel, B. & Vandewalle, J.** (2003). Hardware architectures for public key cryptography. Elsevier Integration, the VLSI Journal, special issue on Embedded Cryptographic Hardware 34(1-2), 1–64.

[33] **Hamilton, W.** (2011). Smart Cards and Biometrics. A Smart Card Alliance Physical Access Council White Paper. 1–26.

[34] **Fernandez, E. B., Pernul, G. & Larrondo-Petrie, M. M.** (2008). Patterns and pattern diagrams for access control. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 5185 LNCS, 38–47.

[35] **Priebe, T., Fernandez, E., Mehlau, J. & Pernul, G.** (2004). A Pattern System for Access Control. Res. Dir. Data Appl. Secur. XVIII 144, 235–249.

[36] **Sandhu, R. S., Coyne, E. J., Feinstein, H. L. & Youman, C. E.** (1995). Role-Based Access Control Models. IEEE Comput. 29, 38–47.

[37] **Sandhu, R. S., Ferraiolo, D. & Kuhn, R.** (2012). The NIST Model for Role-Based Access Control: Towards A Unified Standard. 5th ACM Workshop on Role Based Access Control 47–63.

[38] **Ye, N., Zhu, Y., Wang, R. C., Malekian, R. & Lin, Q. M.** (2014). An efficient authentication and access control scheme for perception layer of internet of things. Appl. Math. Inf. Sci. 8, 1617–1624.

APPENDICES

APPENDIX A

The Confirmation codes of the fingerprint sensor:

00h: commad execution complete
01h: error when receiving data package
02h: no finger on the sensor
03h: fail to enroll the finger
06h: fail to generate character file due to the over-disorderly fingerprint image
07h: fail to generate character file due to lackness of character point or over-smallness of fingerprint image
08h: finger does not match
09h: fail to find the matching finger
0Ah: fail to combine the character files
0Bh: addressing PageID is beyond the finger library
0Ch: error when reading template from library or the template is invalid
0Dh: error when uploading template
0Eh: Module can¡t receive the following data packages
0Fh: error when uploading image
10h: fail to delete the template
11h: fail to clear finger library
15h: fail to generate the image for the lackness of valid primary image
18h: error when writing flash
19h: No definition error
1Ah: invalid register number; 21.
1Bh: incorrect configuration of register
1Ch: wrong notepad page number
1Dh: fail to operate the communication port
Others: system reserved

APPENDIX B

Display object constants:

```
#define GENIE_OBJ_DIPSW           0
#define GENIE_OBJ_KNOB            1
#define GENIE_OBJ_ROCKERSW        2
#define GENIE_OBJ_ROTARYSW        3
#define GENIE_OBJ_SLIDER          4
#define GENIE_OBJ_TRACKBAR        5
#define GENIE_OBJ_WINBUTTON       6
#define GENIE_OBJ_ANGULAR_METER   7
#define GENIE_OBJ_COOL_GAUGE      8
#define GENIE_OBJ_CUSTOM_DIGITS   9
#define GENIE_OBJ_FORM            10
#define GENIE_OBJ_GAUGE           11
#define GENIE_OBJ_IMAGE           12
#define GENIE_OBJ_KEYBOARD        13
#define GENIE_OBJ_LED             14
#define GENIE_OBJ_LED_DIGITS      15
#define GENIE_OBJ_METER           16
#define GENIE_OBJ_STRINGS         17
#define GENIE_OBJ_THERMOMETER     18
#define GENIE_OBJ_USER_LED        19
#define GENIE_OBJ_VIDEO           20
#define GENIE_OBJ_STATIC_TEXT     21
#define GENIE_OBJ_SOUND           22
#define GENIE_OBJ_TIMER           23
#define GENIE_OBJ_SPECTRUM        24
#define GENIE_OBJ_SCOPE           25
#define GENIE_OBJ_TANK            26
#define GENIE_OBJ_USERIMAGES      27
#define GENIE_OBJ_PINOUTPUT       28
#define GENIE_OBJ_PININPUT        29
#define GENIE_OBJ_4DBUTTON        30
#define GENIE_OBJ_ANIBUTTON       31
#define GENIE_OBJ_COLORPICKER     32
#define GENIE_OBJ_USERBUTTON      33
```

CURRICULUM VITAE

Name Surname:	Sercan Aygün
Place and Date of Birth:	İzmir 19/06/1989
Address:	Yıldız Teknik Üniversitesi, Elektrik Elektronik Fakültesi, Bilgisayar Mühendisliği Bölümü, D Blok, Oda: B-026, Davutpaşa Mah., 34220, Esenler-İstanbul TÜRKİYE
E-Mail:	ayguns@itu.edu.tr sercan@ce.yildiz.edu.tr
B.Sc.:	Eskişehir Osmangazi University, Electrical-Electronics Engineering, 2013 Eskişehir Osmangazi University, Computer Engineering (Double Major), 2013
Professional Experience and Rewards:	Research Assistant, Yıldız Technical University, Computer Engineering Department, Hardware Division, since 2014 October

List of Publications and Patents:

Güneş, E. O., **Aygün, S**., Kırcı, M., Kalateh, A., Çakır, Y., - & (2014, August). Determination of the Varieties and Characteristics of Wheat Seeds Grown in Turkey Using Image Processing Techniques. Agro-geoinformatics (Agro-geoinformatics 2014), Third International Conference, (pp. 1-4), Beijing, China.

Aygün, S., & Akçay, M. (2015). MATLAB Paralel Hesaplama Aracı ile A* Algoritmasının Rota Planlama için Analizi Genç Mühendisler Sempozyumu 2015. Türk Mühendisler Birliği, Mayıs 2015, İstanbul, Türkiye

PUBLICATIONS/PRESENTATIONS ON THE THESIS

Aygün, S., Akçay, M., & Güneş, E. O. (2015). Bulut Sistemler için Önerilen Biyometri Tabanlı Güvenlik Sistemine Genel Bakış. The Third International Symposium on Digital Forensics and Security (ISDFS 2015), Ankara, Turkey.