2011

Smart access control system with behavioral profiling and dynamic PIN concept

Lohit Penubaku
Louisiana State University and Agricultural and Mechanical College

SMART ACCESS CONTROL SYSTEM WITH BEHAVIORAL PROFILING AND DYNAMIC PIN CONCEPT

Thesis

Submitted to the Faculty of
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Department of Electrical and Computer Engineering

by
Lohit Penubaku
B.E., Visvesvaraya Technological University, Bangalore, India 2005
M.S.E.S., Louisiana State University, Baton Rouge, USA 2011
August, 2011

Acknowledgements

I am pleased to thank many people who made this thesis possible. I cannot imagine completing this thesis without their generous help. I will remember, and appreciate their consistent support forever. I would like to deeply thank my advisors Dr. S. S. Iyengar and Dr. Xin Li. They enhanced my confidence, motivation, and always inspired me. Without their support I could have never completed this thesis. I am deeply grateful to Dr.Wu, both for his support and trust, in me and my work. Once again I would like to thank them all for being on my committee.

My special thank to Jung-Hoon Kim for being a mentor, friend and brother without whom this thesis would never have got completed. I would also want to thank his wonderful wife Keyyoung for supporting him and for the wonderful food that she prepared while we worked on late nights. I would like to thank my friends, Gustavo, Rajesh, Praveen, Gokarna, Karthik, Bala, and everyone else in the US and back in India for believing and supporting me. A special thanks to loved ones and all the people who made my life in Baton Rouge wonderful.

Finally, I would like to give great appreciation to my family. They always gave me unquestioning faith and encouraged me in every time. Especially, My father and mother for everything which cannot be put into words. Despite their physical absence, their love and backing has helped me in the successful completion of my study at LSU. I cannot end without mentioning my siblings Chaitra and Manav for bearing me and making me their roll model.

Table of Contents

List of Tables

List of Figures

Abstract

Since ancient time, an access control device has been used for securing valuable properties as well as lives from threatening people. The most representative security device is Lock/Key. Recently, those security device technologies have been improved tremendously and provided various types of security methods. Nevertheless, these methods are not individually perfect to provide optimal security. Therefore, in recent years, many such methods have been combined and used together to provide the required level of security. However, such combination can enhance security for limited number of users only, but very difficult to provide scalable security with the number of users increases. These methods, most of the time, are not convenient for wide range of users (i.e., the innocent users who do not pose any threat) due to access time delay and different layers of authentication.

We believe that our security system should exhibit capabilities that support adaptive security procedures for different range of users so most innocent users require minimum layer of identity authentication and verification while suspicious users may require to pass through some additional layers of security authentication and verification. These capabilities enable the system providing enhanced security as well as convenience to the users. A natural question in providing enhanced security is how to categorize certain individual users who require additional layers of authentication. We address this question by proposing a novel smart access control (SAC) system which can identify and categorize suspicious users from the analysis of their behavioral activities and bio-information.

The SAC system observes and records users daily behavioral activities and uses those activity patterns for providing adaptive security. From the analysis of the collected data, it selectively chooses certain users for additional layers of authentication procedure and quickly isolates those individuals who might pass thorough scrutiny by security personnel. Due to this adaptive feature, the SAC system not only minimizes delays and provides more convenience to the users but also enhance the security measure, at the same time. Moreover, we propose a novel idea of dynamic non-physical key: a concept that uses individual user's

memory and brain power to generate and update his security key dynamically so that the key keep changing with time without the need of additional devices.

In this thesis we will show the feasibility of the SAC System with implementation of the system along with its prototype implementation. We also validate the system by presenting some experimental result.

Chapter 1

Introduction

The safety of property is the top priority of many organizations. Organizations are working on providing secure access to their resources in order to prevent any kind of loss to the organization. Providing special privileges to their employees can prevent this loss. Access control mechanism is used to protect both the resources and the personnel. One of the most important techniques to implement this kind of security is the door security. Various mechanisms have been developed to provide secure access to the area. The access to such kind of systems can be categorized into physical and non-physical keys. The physical access keys include situations where the user has been provided with some physical entities such as lock/key, smart cards like RFID, magnetic strips, biometric etc. The non-physical keys are more like entities that cannot be touched or seen, for example PIN, password, behavioral, etc.

Physical and non-physical keys have been useful in providing secure access to the resources. However these methods are not individually prefect to provide optimal security. The methods are also not user friendly and are not convenient to use for most of the users. Therefore, the proposed SAC system will support adaptability features and provide minimum layer of authentication for the legitimate users and making it difficult for inappropriate users to pass though the security system.

The heart of the SAC system is to observe and record daily activities of the users and eventually use those activity to create patterns for providing security adaptiveness. After conducting experiments and analyzing the data, the system selectively chooses suspicious users for additional layer of security and isolates those individuals who might pass the scrutiny. Due to this adaptive feature, the SAC system not only minimizes delays, it also provides more convenience to the users and enhances the security measure at the same time. The SAC system also uses the novel idea of dynamic non-physical key, which makes use of the users memory and brain power to generate and update their security key dynamically so that the key keeps changing with time, without the need of additional devices.

Chapter 2

Background

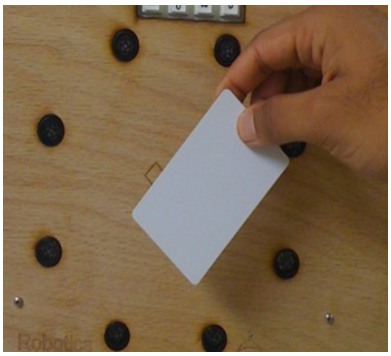
Security has been of major concern now a days, and the proper security must be provided for access into secure area. Different methods have been proposed to provide secure access to those areas, such as voice recognition, face recognition system, secure cards, secure PIN and many others. The main purpose of these access control systems is to verify the legitimate users and provide access to the required resources. The access control systems map the resources to appropriate users. All these access control techniques have been helpful in many aspects, but there are some situations where these techniques can be easily breached and failed to provide security. We will look at these methods with respect to two parameters: Physical and Non-Physical keys.

2.1 Physical Key

Physical key are entities that are physical in nature, meaning things that can be felt. Traditional keys which come with a lock is a physical key. These are something additional that people carry along with them all the time either to get into their apartment or their car. All such traditional keys can be put into access systems called Traditional Access Control system (TAC). Apart from this, there are other physical keys that are electronic in nature, called Electronic Access Control (EAC). Smart cards, IC, and RFID cards are all electronic physi-

cal key that user carry with them to get access into a secure area. We give brief description of each of them below:

(a) TAC



(b) EAC

Figure 2.1: Physical Key

2.1.1 Traditional Key

The keys that have been used for centuries are still being used as an instrument to operate a lock. A key is a piece of metal which has a blade and a bow. The blade goes into the keyway of the lock. A lock will have a number of levers inside positioned in a unique way. The key blade is cut in such a way that it matches the design of the lock. When the key is turned, the levers in the lock align and releases the bolt in the lock. This means there can be multiple keys for just one lock. This is a major drawback of the key, if someone steals the key he will have access to locked area. It will eventually be difficult to find out if something went missing that the lock was used to protect, and in these days there are many ways to clone the key or even to break a lock.

2.1.2 Smart Cards

The use of smart cards is the most general secure access technique used by many organizations. Most recently, smart card access system uses the Internet as a central control system. The main objective of the system [6] is to protect the resources from inappropriate users.

Each door has an access control point, which is connected to the server and this takes care of the access. The users are given access by using the smart card, which contains the users unique identity. This system fails to consider the situation of stolen, duplicated, forgotten, lost or impersonated cards with accuracy. This is very important aspect to be considered since theft is a frequent and easy way to gain access to a privileged areas.

Method: Each door is connected to a Control Access Point (CAP), which are connected to a server through the Internet. The server takes care of the access to the user according to the access policies. There is no specific learning in this method. All the credentials of the user are stored in a database manually, which contains the user privileges and the data regarding the user.

2.1.3 Voice Recognition

The research on security access control systems led to the improvement of voice recognition techniques. Astuti [1] provides a technique, which uses the voice of the user to provide access. Secure Access control is the main objective of this project. This paper mainly concentrates on overcoming the general smart card-based access system. This papers states that among all the biometric techniques, voice has the best characteristics and usability. The access to the room is provided by authorization by the means of a microphone attached to the system. The proposed system uses feature extraction technique from the users voice and then an Adaptive-Network-based Fuzzy Inference Systems (ANFIS) is used to develop models of the authorized persons from the feature extracted from the authorized person. This technique has been tested with researchers in an isolated laboratory. The voices of these researchers are recorded over and over again till the models learns. This shows that the training is a very time consuming process and general users do not prefer spending too much time on verifying themselves. The researchers do not mention about the external noise and health conditions. The recording of the voice by the researchers can be affected by the external noises, which may result in recording the voice again and also it may affect the users at the

time of login if there are any external noises. This is an important aspect to be considered for secure access into a room.

Method: This system does learning in two phases. The first phase is the training phase, which involves feature extraction, authorized person modeling, and authorized person database. The feature extraction module takes care of converting the raw voice into feature vector. And then determine the premise parameters. Followed by the training of the ANFIS using the input pattern and desired output, and finally the validation of the tested data. This is how the system learns and adapts to the new users.

2.1.4 Fingerprint

Another Biometric technique, which is generally used in access control systems, is the use of Fingerprints. This is another common technique, which is used to provide access to the legitimate users. This technique aims at overcoming the traditional problems of mechanical locks, such as lost key and personnel transfer. In fact, [10] provides a technique, which uses this kind of technique to provide access to the users. This access control system combines the Fingerprint vault scheme and IC card technique. This model stores the information related to the legitimate user's fingerprint in his IC card, which is bound to the user. Event though the authors state that, the loss of card does not give an opportunity to gain access to the room, the author does not specify the situations where the user finds it difficult to login due to sweat in his hands or situations where there is a cut to the users fingers. These are quite common and should be considered while designing the model.

2.1.5 Facial Detection

Facial detection is an important technique in providing access to the room. [7] provides a facial detection technique, which is used to check the genuine users. Junfeng et al. [7] suggests a technique, which overcomes the problem of general 2D face recognition technique, that may fail with illumination, pose, expression, make up and age. This paper has developed a 3D

face detection system, which emphasizes shape, texture, and skin color of the face. They have proposed a skin color information and depth date if human face factor for detection and PCA (Principal Components Analysis) algorithm for recognition. Various experiments have been done, where the author finds that illumination, expressions and mechanical vibrations may affect the recognition accuracy. These factors affect the system significantly and the user may find difficulty in accessing the system.

2.2 Non-Physical Keys

This can be defined are keys that one does not carry a key physically. We saw in traditional key case that there might be N same keys for one lock. In non-physical key case, we have N different keys for one lock. One good example could be a pin controlled lock. Some of the other non-physical keys can be memory based keys like password, secret questions, etc., and a few biometric and behavior of an user are also considered as non-physical key.

2.2.1 Color PIN

De Luca et al. [2] proposed ColorPIN, an authentication mechanism that uses indirect input to provide security enhanced PIN entry, and showed that it is notably secure than Static PIN entry. Later they conducted a field study, which showed a big influence of contextual factors on security and performance in PIN based ATM authentication and need for the design of alternative ATM authentication mechanisms that are resilient to distraction and social compatibility.

2.2.2 Password

Passwords are the most basic way to provide security in access control system. But these passwords can be hacked and can be misused by others. In order to provide more security, the type of characters to be used for a word to act as a password has been restrained

and made more unpredictable. Different combinations of characters including alphabets, numbers and symbols are generally used to make difficult for the illegitimate in guessing guess passwords. Even though, all these precautions have been taken the passwords are still hacked and misused. There can even be shoulder surfing, by which the illegitimate user eavesdrops while the user types the passwords and misuses it. Hence Dino Schweitzer et al. [9] proposed a technique, which is based on the pattern matching techniques. This proposal relies on pattern of the characters, which changes randomly.

Visualization techniques were also used to collect the data, and used in pattern categorization. This project also checks whether patterns could be classified in common categories. Dataset of passwords including those known to be pattern based are collected and a visualization technique is developed to analyze these passwords for common patterns. Heuristics are developed based on the recognized patterns and a password file is generated. This file is in the dictionary form of the pattern heuristics. Password cracking tool is then applied on the pattern dictionary.

2.2.3 Security Question

This method is yet another technique used now a days for security. This method generally generates a security question if the user forgets his password. This can be seen in any of the web mail accounts. How ever many tests were conducted to test the reliability of the system [8]. Stuart Schecher et al. have tested the reliability on a number of users and their acquaintances. The test included asking security questions to participants and asked their acquaintance to guess the answer. This test resulted in 17% able to guess the answers. The survey also states that 20% of participants forgot their passwords in six months. Moreover, 13% of acquaintances were able to guess the answer to the security question within 5 attempts.

As suggested in the survey [8], this is not reliable as the illegitimate users can guess the answer to the security question of the user, if he knows him. Making it a unreliable method

to provide security.

2.2.4 Behavior

The intelligent access control system based on user behavior [1] states that biometrical sensors are sometimes harmful and likely to cause abuse [6, 10]. This paper presents a high-security access control system, which uses biometrical sensors and several intelligent methods for access control. This method is used to prevent unauthorized users gaining access even if the sensors are by-passed. Further, the system is developed using integration of different sensors and AI modules.

This system involves four sensors [door, card reader, fingerprint reader and camera] and four modules [expert rules, micro learning, macro learning, visual learning]. The user verifies himself with his card with the help of card reader. Then he gives his fingerprint. If the user is verified the doors open and close. The camera and the biometrical sensors monitor this event. Time plays a vital role in recording the information. The attributes such as time between the acceptance of fingerprint and identification card, time between the acceptance of identification and time of door opening and finally the time between the door opening and closing. All these attributes are categorized into macro attributes.

This method used three learning modules. The first sub-module constructs a decision tree using the macro attributes, which is used to explain a decision after a classification. The second sub-module is constructed similar to the first module, but the micro attributes such as behavior of a person, his/her habits and motoric abilities [7]. The final sub-module used Local Outlier Detection for detection of deviant entries [2, 9, 8]. This module helps in circumstances where the entries are not distributed uniformly. After the data is collected, visualization of the data is performed in which normalized value of each attribute from its minimal to maximal values are used.

In the next step, the uniformly distributed values with uninformative attributes are eliminated. These attributes, which have the deviation close to the average standard de-

viation, are eliminated. The results are obtained by combining the weighted voting of the sub-modules. Depending upon the output of these results the values are classified into OK, Warning and Alarm. The value range for OK, Warning and Alarm are obtained from the test data. This is obtained using the k-number of neighbors, which mainly depends upon the test cases and noise in the data. Finally, the integrated macro module recognized 90.85% of irregular entries and produced false alarm in 6% of regular.

Method: Classification is an important task for this project; therefore this project uses Weka and "J 48 algorithm", which is a java implementation of Quinlan's algorithm. Where regular entries are considered as positive learning examples and irregular as negative learning examples. After the classification, decision trees were constructed, with macro attributes in the first module and macro-micro attributes in the second module. The third and the most important module for detecting the deviant entries is done using the Outlier Detection technique.

2.3 Problem Statement

There are a lot of methods proposed to provide security in present state of the art. We previously discussed most of the commonly used methods, and also analyze their drawbacks to provide security which makes the system to be vulnerable. There were many approaches and techniques which showed a lot of potential, but they are not individually perfect in providing optimal security. One of the simplest ways to overcome the drawbacks is to have N-number of methods in one system. But it is a hassle for the users, since he needs to personally go through each method.

After looking into all the present systems and their drawbacks, we have to come up with a system that could overcome the drawbacks in the present system. This can be made possible by making the system intelligent and adaptive in real time. To achieve this, the system observes and record user's daily behavioral activities and uses these activities to

create patterns for providing adaptive feature for our security. With the help of this adaptive feature, the SAC system helps in minimizing the delay (time taken to get access) for each user. This adaptive feature makes the SAC system intelligent, which in turn enhances the security measure, at the same time.

At this point let us put aside all the drawbacks, and look into how we achieved intelligent and adaptive system. First, we will look at our proposed system architecture, and talk about its generic features and robustness. Finally we will see how we used the architecture in our implementation to prove the system architecture.

	Smart Card						Biometric					
							Physiological				Behavioral	
Characteristics	Embossed	Magnetic	Integrated circuit cards	Memory cards	Contactless smart cards [RFID]	Optical Memory Cards	Face recognition	Finger	Hand Geometry	Iris	Voice	Signature
Universality	Duplicated	Duplicated	Duplicated	Duplicated	Duplicated	Duplicated	Duplicated[twins]	No Duplication	No Duplication	No Duplication	Duplicated[Recorded]	Duplicated[forged]
Uniqueness	high	high	high	high	high	high	Medium	high	Medium	Very high	high	high
Permanence	medium	medium	medium	medium	medium	medium	Low	Medium	Medium	High	Low	medium
Collectability	NA	NA	NA	NA	NA	NA		High	Medium	Low	Low	medium
Precision	High	High	High	High	High	High	Medium	High	Medium	Very High	Medium	Medium
Simplicity	high	high	high	high	high	high	Low	high	Low n	Low	Medium	Medium
Cost	Low	medium	medium	medium	High	High	Low [<$50]	Medium [<$200]	Medium [<$500]	Very High [>$3000]	Vey low [<$5]	Medium [<$300]
Exclusivity	High	High	High	High	High	High	Low	Low	Medium	High	Low	medium
Convenience	High	High	High	High	High	High	Medium	High	Medium	Low	Medium	High
Acceptability	High	High	High	High	High	High	Medium	Medium	Medium	High	Medium	Medium
Storability	NA	NA	NA	NA	NA	NA	High	Medium	High	Very high	High	medium
Susceptibility												
Error correction	NA	NA	NA	NA	NA	NA	Medium	High	Medium	Low	Low	medium
Scalability	NA	NA	NA	NA	NA	NA	Medium	High	Low	Very high	Low	High
Maturity	NA	NA	NA	NA	NA	NA	Medium	Very high	High	Medium	Medium	Medium
Sensor type	contact	contact	contact	contact	contact	Unobtrusive	Unobtrusive	Contact	Contact	Unobtrusive	Unobtrusive	Contact
Sensor Size	Medium	Medium	Medium	medium	Medium	high	Small	Small	large	Medium	Very small	medium

Table 2.1: Comparison Table of Possible Systems

Chapter 3

System Architecture

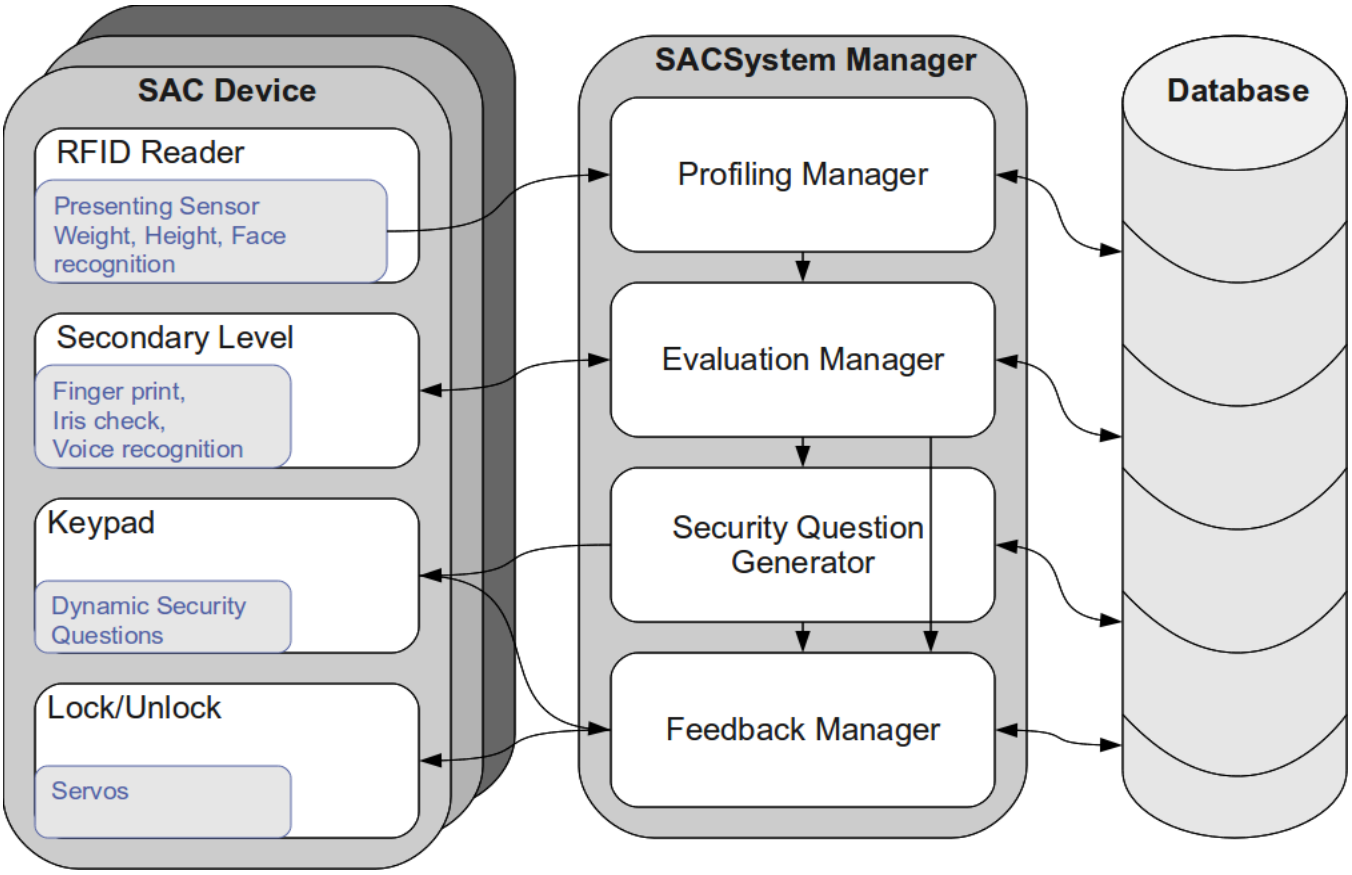


Figure 3.1: System Architecture

The architecture that we proposed has three modules: device, manager and database. One can use these modules in any way they want. The device module is a standalone device.

It basically holds all the hardware together. In simple this can just be a lock or a card reader. The manager and database module can be made one module or they can work individually. Both these modules are used to evaluate users and storing information non-physical key in database. Communication protocol can be used to communicate between device-manager and manager-database.

3.1 SAC Device

This module holds all the hardware that is needed for the system. If we have to compare this with the present systems then the best example would be a simple access control system with just a RFID reader, a keypad and a lock. The architecture that we developed can hold N-Hardwares in one SAC device. We can categorize the hardwares based on the requirements and functionality for the device. They can be categorized as follows:

3.1.1 Primary Level Hardware

The primary level can have a number of different devices. All the devices that are of primary requirement for a security system can be included in this part of the system. The devices in this level are the minimum requirements for the basic authentication process for the system. A simple traditional key can be considered as primary device hardware, since it is the minimum requirement to open the door for the respective lock. The other devices can be RFID card, Smart card, IC card, etc. all of these are also called digital keys. Other than the traditional key, we can see that our system architecture can be used for a simple electronic access control system with just the primary level hardware in the SAC device module and with the rest of the modules unchanged. We will look at two different systems that are possible to setup with our architecture at end of chapter.

3.1.2 Secondary Level Hardware

The secondary level can have many more devices to improve the security feature of the system. This particular level can be used whenever heavy security is needed. Some examples include the system used in the White House, FBI, CIA, etc. However, the secondary level may be optional, when required system needs to be less complex and cost effective. The purpose of the secondary level is just a backup for providing additional security. In general when considering a traditional key and lock system there is no secondary level in the system. In the past people used the second lock in the system as their secondary level of security. The other advanced secondary level devices can be: fingerprint reader, iris scanner, speech recognition device, etc. We have already seen a few drawbacks of the advanced secondary level devices individually.

3.1.3 User Interactive Level Hardware

The user interactive level hardware provides interface between user and the hardware. All the security features of the system can be implemented in this level. A few of the hardware can be analog key dial, touchpad, keypad and LCD display.

3.1.4 Lock/Latch Hardware

All the security access systems should have a mechanical contraption attached to the system. The most used hardware is a lock, and the other more advanced hardware is the latch system and the magnetic lock system.

3.2 SAC Manager

The SAC System manager can be called the brain of the whole architecture. Here the data from the SAC Device is processed by one of the sub managers of SAC manager based on the kind of information received from the SAC device. The SAC manager is a daemon

process that runs continuously. The manager communicates not only with the SAC device but also with the database. There can be a number of different ways of communication between the device and the manager based on the SAC device requirement. The manager then decides on which sub manager to use, based on the data received. The sub manager in turn communicates with the database to read and write data for specific processing. We will look into each of the sub managers in detail as to know how they can be used.

3.2.1 Profiling Manager

The main purpose of the profiling manager is to handle all the data pertaining to a particular user profile. The kind of data that is stored for the user can be different based on the security system. The different kind of data can be a traditional key, an user ID (RFID, IC card, etc.), password, pin, behavioral pattern, weight and height, skin color, tracking path and biometric information (face recognition, iris, hair color, etc.). All of these user profile data needs to be stored somewhere or the other, and the best place to this is on a database.

The profiling manager can constantly communicate with the database to perform operations like updating the database, retrieving information from the database, and also requesting evaluation of the profiling data for the user from the sub managers. All of the data that goes into the database is very essential for identifying different users in our system. This architecture uses the profiling data for learning different users with respect to behavioral change.

3.2.2 Evaluation Manager

One of the main purposes of our system is to differentiate users with respect to their behavioral patterns. The evaluation manager evaluates data of the user received from the device, with the profiling data that was stored in the database by the profiling manager. The evaluation manager does a variety of evaluations based on the primary level and secondary level hardware, along with requirement of the security system. The evaluation manager not only

evaluates the data but also has to decide what it needs more for identifying the right user.

The evaluation manager evaluate data such as user ID provided by the primary level hardware. The manager then evaluates further on other information like behavioral data also provided by the primary level hardware. If the manager is unable to decide the legitimate user with just the primary level, then the evolution manager requests for advanced profiling information from the secondary level hardware. Most of the database transactions are handled by evaluation manager. After all of the evaluation is done, the manager updates the profiling data of the user for learning and future evaluation.

3.2.3 Security and Feedback Manager

Both security and the feedback manager are controlled by the evaluation manager. The security manager communicates with the SAC device for user interactive task. The roll of the security manager is to request additional security information from the user, on request by evaluation manager. The information can be requested either from primary level hardware or the secondary level hardware.

We can clearly observe that there are multiple transactions take place for one evaluation request between the SAC manager and the SAC device, and between database and the SAC manager. If there are N-SAC devices then there can be N-client, and someone needs to keep note of these transactions. To handle this the feedback manager can be used. The feedback manager is the one which decides whether to allow access or deny access. The feedback manager also maintains a log table in the database.

3.3 Operational Procedure

We have seen all the key features of the modules, and now let us look at how the system architecture operates, with the help of a flow chart. The user needs to present his primary level ID to the SAC device. The user ID read from SAC device is sent to the SAC manager.

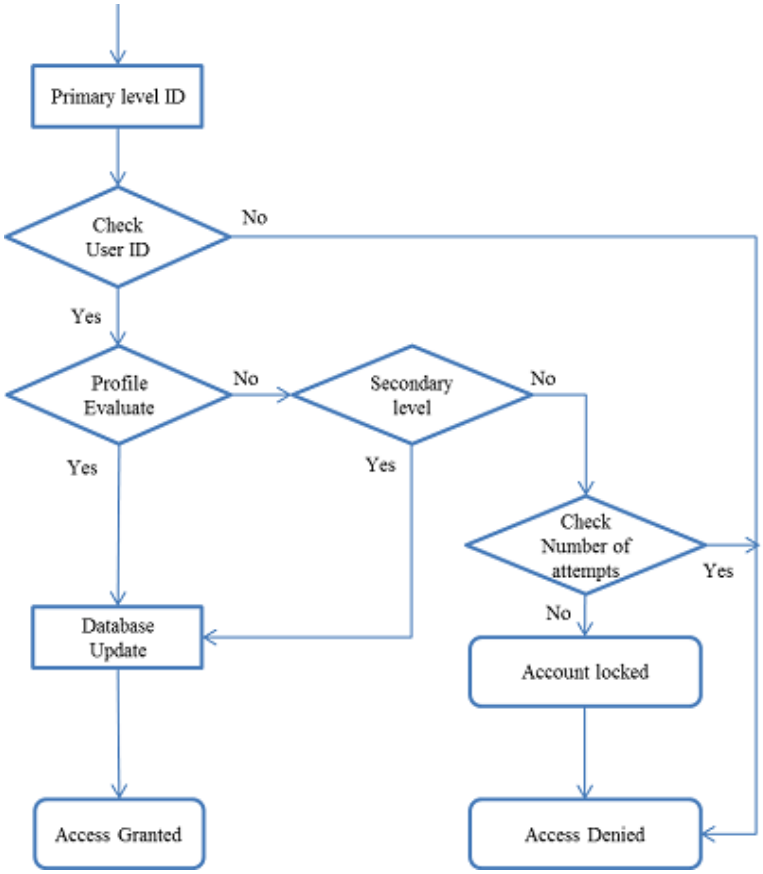


Figure 3.2: Generic Flowchart

The manager then evaluates the data received to see if the user exists in the database. If the user ID does not match to any entry in the DB it waits for a few seconds before it can acknowledge access denied. But if the user exist then the SAC manager evaluates the additional data received from the primary level hardware which is sent by the SAC device to the manager. The manager uses this data to evaluate profiling data previously created in the database for the user. We can make note here that the feedback manager is responsible for maintaining connection between modules at all time.

If the data matches, the manager updates the database with the latest profiling data for the next evaluation for the same user. This is the point where the system learns about the user which helps improve the precision of the system. If the profiling evaluation fails then the user will be put through secondary level of security check, here the user input is required.

The data received from the secondary level then goes through the evaluation process. If the user clears the secondary level then the manager updates the profiling data and allows access for the user. If the user fails the secondary level check, the manager checks the number of attempts on the ID and if the attempts exceed five times then the manager locks the user and denies access. If all the decision blocks say "yes" then the manager learns/updates database and says access granted. We can clearly see that the system keeps updating the database which helps in behavioral learning of the user

3.4 SAC Architecture Based System

3.4.1 Simple SAC System

Our system architecture can be used to develop a simple access control system to an advanced access control system. The simple system can just have a RFID reader and keypad, both together makes our SAC device. The RFID reader can be considered as the primary level hardware and a keypad and the secondary level hardware. These two hardware may be connected to a standalone computer somewhere inside the secured area. This standalone computer can resemble the manager in our architecture. When the user presents the RFID card and the manager will look up somewhere (database/Excel/etc.) to see if the user exists in the system. If the user exists then the manager may request the user to enter a static PIN assigned to the user. We can clearly see how the architecture can be used to create a simple system.

3.4.2 Advanced SAC System

More advanced access control system such as the ones used in FBI/CIA etc. can also be implemented using our architecture. In such places assurance of the right person gaining access into the building is very important. In order to build such system we require a lot of device hardware. Few of the devices at the primary level can be a user ID, keypad, camera

Figure 3.3: Simple Access Control System

etc., and devices at the secondary level can be fingerprint reader, iris check, face recognition system etc. Putting all these all these together makes the SAC device. In such systems there will be a central unit that manages the device, and also a secure database that holds all the profiling information of the user.

Figure 3.4: Complex Access Control System

Chapter 4

Implementation

We saw how our system architecture can be used and also a couple of use case. Now let us see how we used the architecture to implement access control system that could overcome the drawbacks discussed previously. As you can see we have three modules in our implementation, which is similar to the proposed system architecture. All the three modules communicate with each other over TCP/IP. We will look into each of these modules in detail, to get a better picture of how the implementation works. Finally we will look at the work flow of the system.

4.1 SAC Device

The device that we implemented makes use of different varieties of hardware. In our implementation we used primary level, user interactive and lock hardware. All the hardware's are connected to a controller called robostix and this is controlled by a processor called the gumstix. The primary level hardware that we used is a simple RFID reader, sonars and weight sensor. For the user interactive level hardware we used a keypad and for the lock we used the electromagnetic latch. Now let us look at how we used each of these hardware in detail.

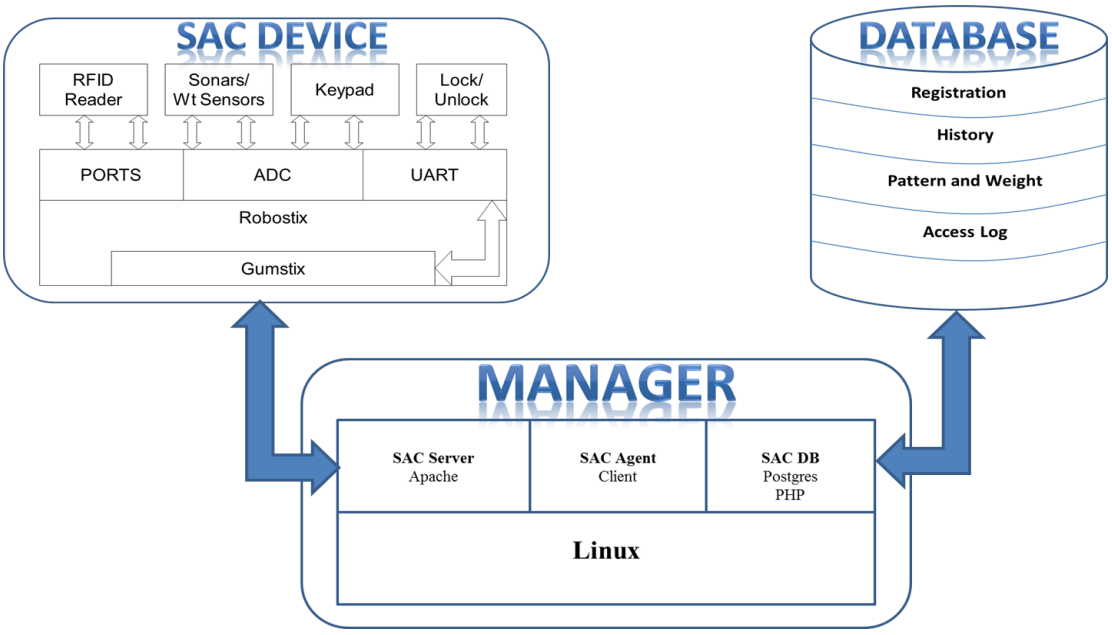


Figure 4.1: Block Diagram

4.1.1 Gumstix

Gumstix is a processor which is based on ARM Architecture, also called single-board computer, which has a similar potential as a tablet PC. Gumstix based products are distributed as both cased packages, which comprises of the required peripherals for communication and also as a single board package, where we only have the motherboard. For a basic Gumstix board the I/O is usually provided using additional expansion boards. The latest motherboard from gumstix is called Verdex and it comes in many configurations with variety of processor speeds and flash sizes.

The purpose of gumstix in our implementation is to do basic data processing and to send processed data to the SAC manager for further processing. The verdex that we are using has a onboard ethernet port which enables us to communicate over TCP/IP. The fact that it runs Linux kernel on it allows us to SSH into the device from anywhere for debugging process. The other reason we use gumstix is because of the robostix that we use is an extension board for gumstix. The key ability of a verdex board is its ability to be a USB host, higher RAM and higher flash memory.

4.1.2 Robostix

Robostix is one of the expansion modules that are designed to accompany the Gumstix in applications. Robostix comes with an AVR ATmega 128 microcontroller with the capability of converting analog to digital, digital to digital, and pulse width modulation. Robostix is a module that will provide the required pins to read data from these sensors, by converting them from analog to digital and then forwarding them to the gumstix. The gumstix is then responsible for sending the information to the manager module. The detailed usage of robostix is available in 7.

4.1.3 Primary Device Hardware

RFID Reader: This is an easy to use RFID reader module. Most of the reader come with an antenna used for receiving ID from a RFID tag. This is a very easy modules to use, all one needs to do is power it on and the reader continuously broadcasts signal. When a user presents the card to the reader, the RFID tag gets activated because of signal and the tag sends its unique ID to the reader. This unique ID is used to differentiate users and helps in creating profiling data for the respective user.

Sonar: Also called as ultrasonic range finders, the way these devices work are that, they use sound waves to calculate the distance. There are a number companies who manufacture them. But the one we used if from Maxbotix [5]. The maxbotix makes one of the most compact, easy to use and reliable sonars. There are two ways to read these sonars, one is through serial interface (RS232) and the other is on analog output. For the detail working of the sonar refer 7. The sonars are arranged around the RFID reader in a particular way so that we can get the presenting pattern of the user. By presenting it is meant as to how the user presents his RFID to the device.

Load Cell: This is a transducer based device, which even the sonar work on. Transducers are devices that when subjected to a force will cause a change in its physical form. One can use this force to calculate energy, which in our case is electric signals. This conversion

is indirect and happens in two stages. Through a mechanical arrangement, the force being sensed deforms a strain gauge. The strain gauge measures the deformation (strain) as an electrical signal, because the strain changes the effective electrical resistance of the wire. A load cell usually consists of four strain gauges in a Wheatstone bridge configuration. Load cells of one strain gauge (quarter bridge) or two strain gauges (half bridge) are also available. The electrical signal output is typically in the order of a few millivolts and requires amplification by an instrumentation amplifier before it can be used.

4.1.4 User Interactive Hardware

The only user interactive level hardware in our implementation is the keypad. The keypad that we used is the classic 4X3 matrix keypad. One may ask why use keypad when they are very vulnerable, the answer to this would be the way we use the keypad. The way we overcame the vulnerability is by using the concept called Dynamic PIN (DPIN). This the most important part of our system which helps in efficient learning.

DPIN: Everyone has a 4 digit PIN that one uses for many purposes. This PIN is called a static PIN as it does not change, but it is unique to each user. The DPIN concept [4] proposed by the RRL group uses the static PIN to compute different PINs with one static PIN making it a dynamic PIN. The way they compute this is by performing mathematical operation on the static PIN using personal information only known to the user. Every time one does mathematical operations it results in a different DPIN. Using this technique in our system we can easily differentiate legitimate from non-legitimate users if the behavioral check were to fail.

4.2 SAC Manager

The SAC manager is a remote server used to control the SAC device and also maintaining the system database. The manager is basically a program that is always running on the

server. In our implementation we used a Linux system as a server. Our server program was completely implemented in C language. The program is split into three different parts SAC agent, SAC server and SAC DB program.

4.2.1 SAC Server

This is a socket program that constantly waits for connection from the SAC device. When the server receives a connection request, it creates a client to send the information over to the SAC agent program. The server can accept a number of connections from multiple devices. When the SAC agent has completed processing the information the server terminates the connection.

4.2.2 SAC Agent

This program is the actual implementation of the SAC manager. All the sub manager functionalities are implemented in this agent program. This program performs multiple tasks based on, how the received information needs to be processed. The agent program frequently communicates with the SAC DB program for evaluating and updating the database.

4.2.3 SAC DB

This can be called a database program as it is written in PostgreSQL C language. This is nothing but a C application programmer's interface to PostgreSQL. libpq is a set of library functions that allow client programs to pass queries to the PostgreSQL backend server and to receive the results of these queries.

4.3 Database

There are a large number of ways to store profile data for a user. For our purpose we had to use a database that is easy to use and reliable. Since the code is written in C language, we

had to look for a database that can be queried in C language. PostgreSQL is the best suited for our needs. The database is not located in the SAC manager system for security reasons. The database has four different tables: Registration, History, Profile and AccessLog.

The registration table holds all the required user information like user ID, address, telephone number, static pin etc. The profile table has only profiling data which is the sensor values from the sonar and the load cells. This information in the table is essential as it holds the presenting pattern and behavioral data. We can see in detail how this table can be used to identify legitimate users. The history table has information of each user transactions such as number of attempts made, access granted, and access denied etc. And finally the access log table tells us about the number of connections made to the database.

4.4 Work Flow

To better understand how the system works we will look at one complete transaction pertaining to the user and the system. In the work flowchart we have divided the jobs

based on the modules. Robostix and gumstix is the SAC device module, and then we have the manager and the database. For the system to work we should ensure that a daemon process is running in the gumstix and the remote server program is also running. Once these two have started the system is ready to be used. Initially the user needs to present his ID, which in our case is the RFID. When the device detects the RFID the robostix reads be RFID along with the sensor values [sonar and weight sensor] and sends it over to the gumstix. The gumstix pre-processes the data received following a certain protocol that is required by the SAC manager. Once the preprocessing is done in the gumstix sense the processed data to the manager.

The manager understands that it is a new transaction based on the data received. The way that it decides is the protocol that gumstix on the server follow. Since it is a new transaction the server needs to check if the RFID exists in the system. To evaluate this

the manager queries the database to see the existence of the RFID. If the RFID does not exist the manager updates the history table for future purpose. Since the RFID does not exist the manager sends access denied to the gumstix and ends the transaction. Once the gumstix receives this information it notifies the robostix saying that the user does not exist. The robostix acknowledges the user "Access Denied" on the LCD screen and keeps the door locked. This is one complete transaction if the user ID does not belong to the system. At this point the SAC device waits until a new user presents his ID.

But if the user does exist the manager evaluates the presenting pattern based on the information sent from the gumstix. The manager checks if there already exists any profiling data by querying into the database. If there is no entry it means that it is a new user ID. Before the manager adds the user profile data to the database, it checks if it is the right user or the fake user. The procedure the manager takes to differentiate between right and fake user is by using the concept of DPIN.

The manager computes the DPIN based on the information of the user is known only to the right user. Once the manager creates the DPIN the manager assigns a new transaction ID, updates the database and sends a "Pin Request" along with the new transaction ID to the gumstix. At this point the manager closes the connection. The gumstix then sends a request to the robostix to acknowledge the user for DPIN, by showing "Pin Request" on the LCD screen. The SAC device waits for a few seconds for the user to input the pin. If the user fails to enter pin the SAC device ends the transaction. If the user enters the pin the robostix sends the pin entered along with the transaction ID that was created by the manager. The gumstix preprocesses this information and sends it across to the SAC manager. Using the transaction ID SAC manager queries the database to retrieve the DPIN that was stored previously.

The manager compares the DPIN on the database and the pin received from the gumstix, if the two match then the manager adds the behavioral data to the profiling data. This data will be used for learning purpose and future evaluation for the user. Once the

manager is done updating the database, it sends "Access Granted" to the gumstix and terminates the connection. The gumstix then asks the robostix to allow access to unlocking and acknowledges the user by showing "Access Granted" on the LCD.

This completes the transaction when the user exists but there is no profiling data. The last possibly case it is, when the user exists and it is profiling data for the user. In this case it the RFID exists the SAC manager evaluates the behavioral pattern by querying into the database. If the behavioral data match's with the new received data from the SAC device, then the manager acknowledges the gumstix to allow access. But if the data received from the SAC device does not match, the manager takes be DPIN and procedure as discussed above. This process continues for every transaction.

We can clearly see that the user interaction with the device is minimal. When the user presents the RFID and if the behavioral pattern does not match, is the only time the user will be requested for DPIN. The manager keeps regarding the behavior data of the authenticated user to learn the behavioral pattern of the user to increase the accuracy and save time.

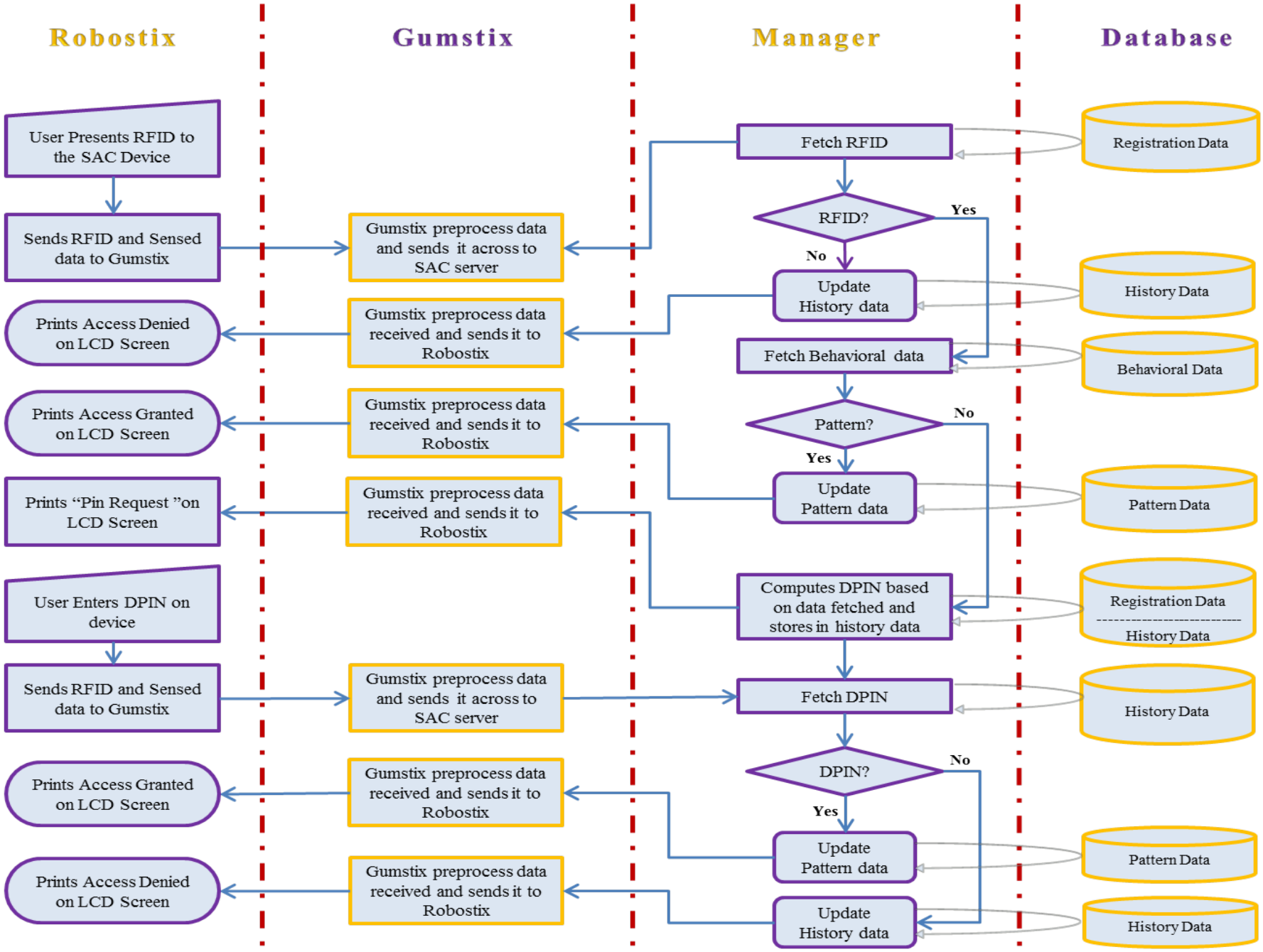


Figure 4.2: Work flow diagram of the System for One Evaluation Cycle

Chapter 5

System Evaluation

5.1 Installation

Let us look at the prototype and the data collected in the database. Below are a couple of pictures of the final working prototype, we can clearly see how the device is setup 5.1. We have the sonars in circular fashion to collect the presenting pattern as efficiently as possible. Then we have the keypad for secondary level authentication where the user ID matches but not the pattern, and the LCD screen for acknowledgement purpose. Figure 5.3 is a prototype of the weight sensor that we built in the lab, which is visible on the floor.

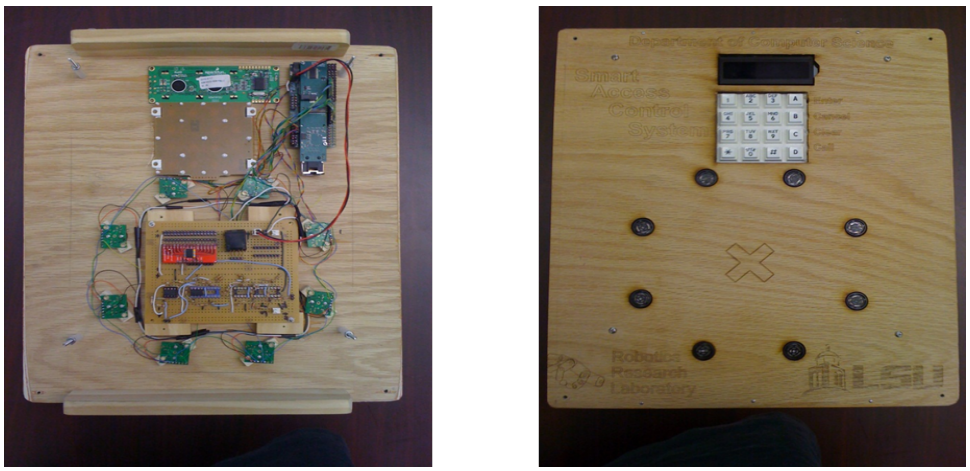


Figure 5.1: Final Prototype

Once we complectly built the prototype of the SAC system. We integrated the prototype of SAC system with the entrance system of the RRL Lab to evaluate the performance of the SAC architecture. We then asked a number of user to test the SAC system. In the testing process we could visually notice that the presenting pattern are quite different among users. At the bottom of Figure 5.3 we can see three different ways people present RFID.

5.2 Analysis

When the user presents the RFID card to the system, the program starts evaluation process, continuously communicates with the SAC device, updates, and validates information on the database. Below are screenshots of the database that show how the SAC system stores data for learning and analysis purpose. Figure 5.4 shows all the tables in our database and the registered users who have access to the lab. Figure 5.5 is the screenshot of the presenting patterns collected and the history table which is the most important tables for the system to learn the behavior of the user.

In figure 5.4 we see in the top portions all the tables that the system makes use for evaluation. The registration table has the basic information of all the users who have access to the lab. Figure 5.5 top part shows what kind of information can be stored in this table.

We were able to see visually how different users have different presenting patterns. But the system can not see visually, hence the system records the distance between the hand and the sonar to create a data pattern that the system uses for evaluation. Figure 5.4 bottom portion shows how the patterns are stored in the digital form. Whenever a user presents RFID, the pattern data is collected and stored in this table. Based on the final evaluation the system marks valid or not valid on the pattern data stored.

For every transaction the SAC manager updates the history table. This table helps in keeping track of the user request in between transaction using the TID created at start of evaluation. Figure 5.5 shows information that can be stored in this table. We can clearly see

Figure 5.2: Installation in Use

the PIN keeps changing because of the DPIN concept. We can also see how it updates based on the evaluation. Keywords like "Pin Request" means SAC manager is requesting for PIN and the respective DPIN is also stored in the table. Keywords like "Denied", "Success" and "Granted" are the decisions made by the SAC manager to keep track of the user request.

Figure 5.3: User using the system

Based on these decisions the SAC manager updates the profiling table to validate between good and bad presenting patterns.

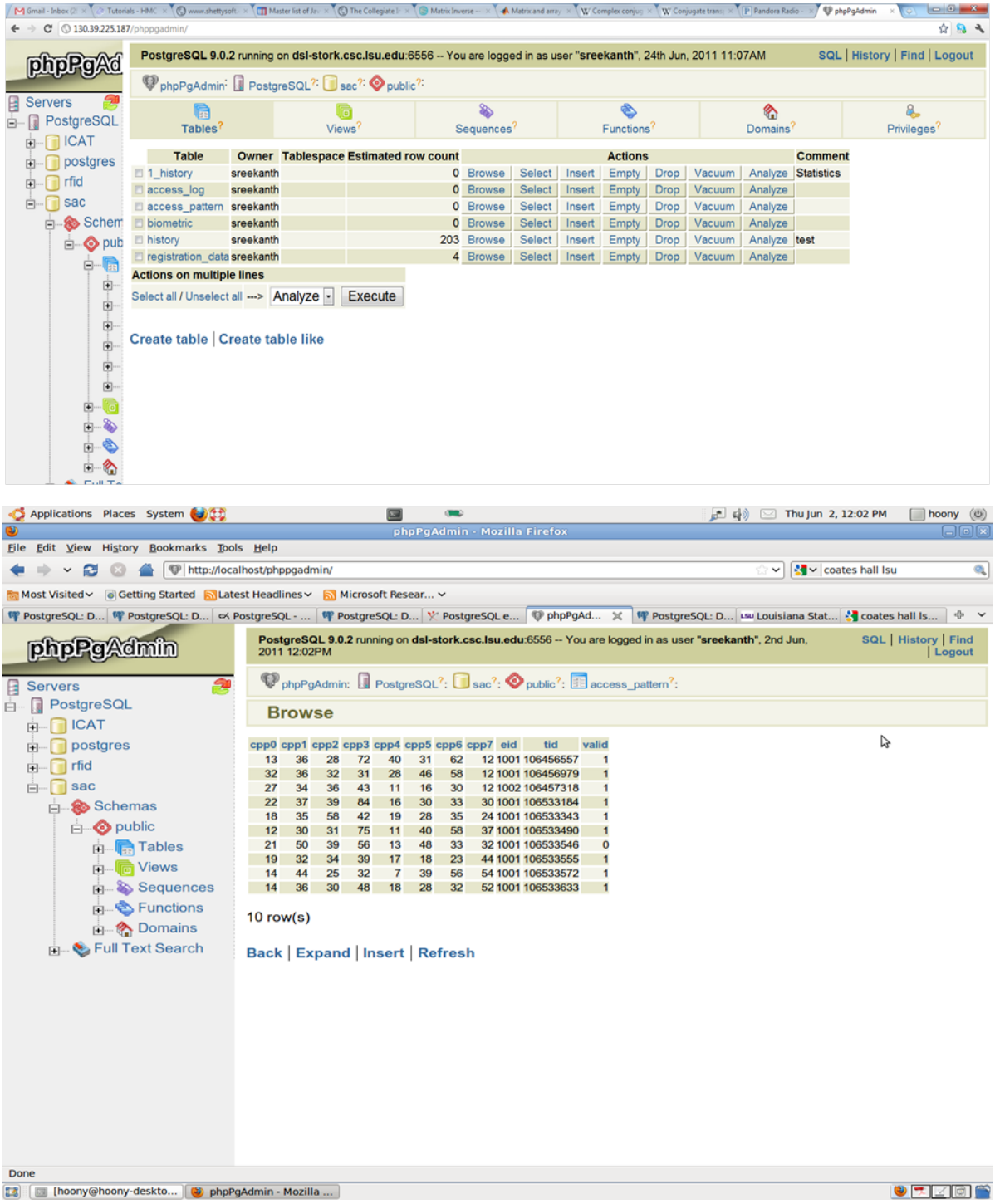


Figure 5.4: All the Tables in Database and Profiling Table

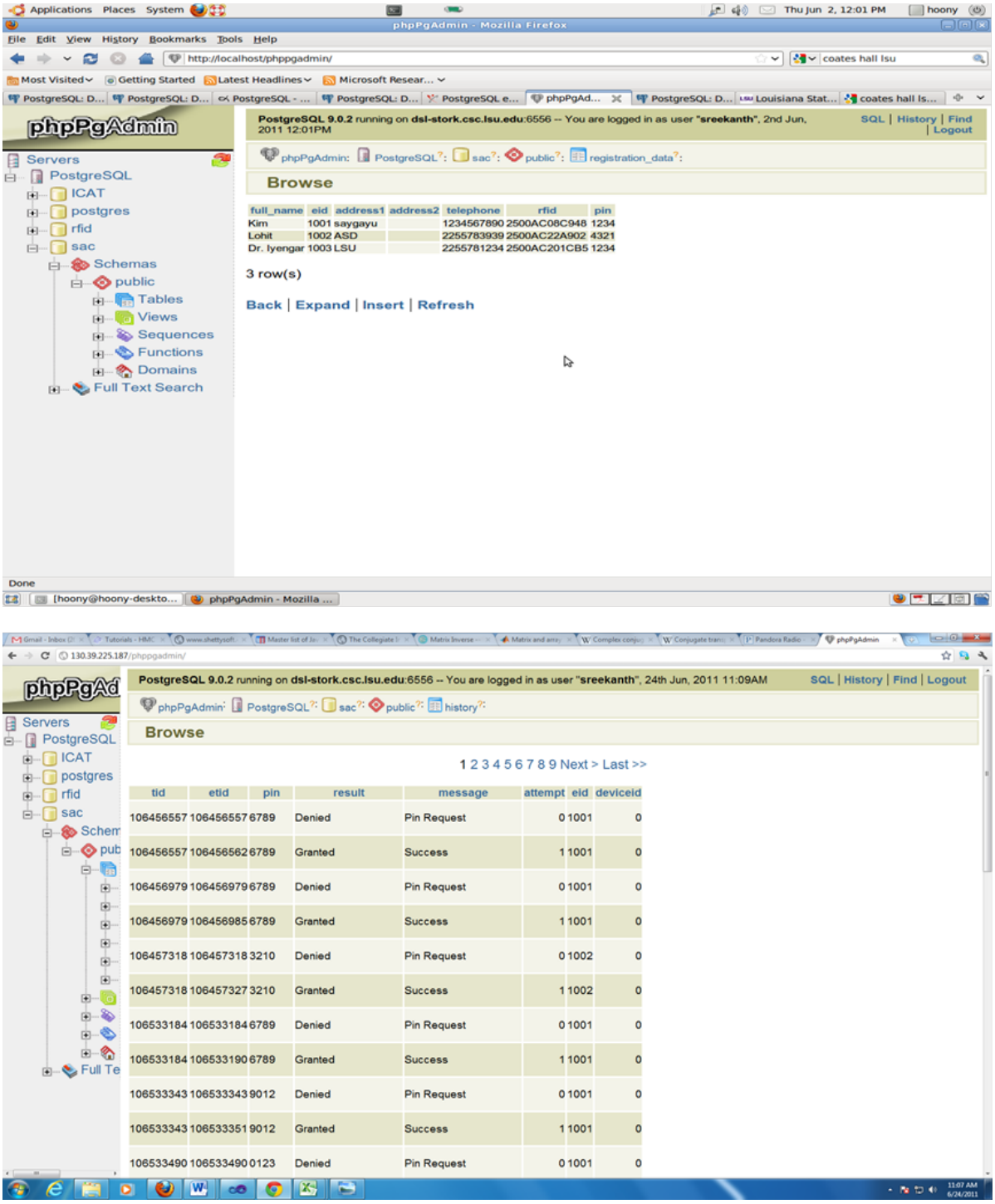


Figure 5.5: Registration and History Table

Chapter 6

Discussion

6.1 Initiative

After looking into present systems, we had to come up with a system that could overcome the drawbacks in the these systems. In this thought process we observed a potential in the human behavior. This initiated our thought process as to how we can capture behavioral habit of a person. We looked into a number of devices that could capture behavioral habits, but unfortunately where not able to find any good and easy to use devices. This got us to think of ways to create our own behavioral habit using devices readily available, for which we found Sonars (ultrasonic devices). We used the sonars to create a presenting pattern for each user. In our system we used RFID as a presenting item. We arranged the sonars around RFID reader as shown below; with this setup we were able to differentiate users with the way they present the RFID card.

The figure above is the state of the sonars when the device is in idle. When the user presents the RFID the devices is initiated, and we find a change in the values of the sonars. With this change we record the pattern as part of user profiling, below are a few patterns that we expect. After we implemented this with the proposed architecture, we found a drawback in using sonar for the system. As we can see from the below patterns that two users may

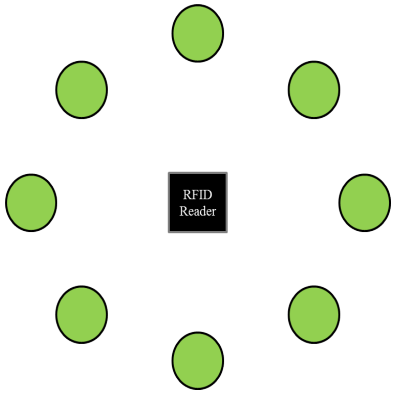


Figure 6.1: Sonar in Idle State

have the same pattern. This got us thinking how we can further differentiate users, and then we decided to use weight as a parameter to differentiate users.

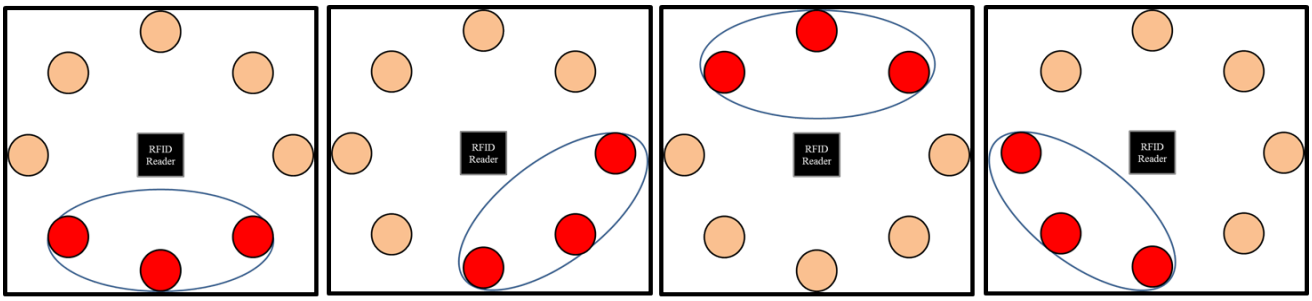


Figure 6.2: Few Expectable Patterns

The addition of the weight sensor increased the efficiency of the system a lot. One thing that you need to observe is that the user is not actively involved in the whole process. All that the user does is present his card to the system and the rest of the process is carried out without the user knowledge.

While we were looking at data of the presenting pattern we came across another parameter which can add up to the decision making process. We can see from the figure on the left side, initially we considered only the distance from hand to device got from the sonars. But the sonars where able return the position of the body as well. Using this we can know the distance between the hand and the body. This also is unique to a user as people may

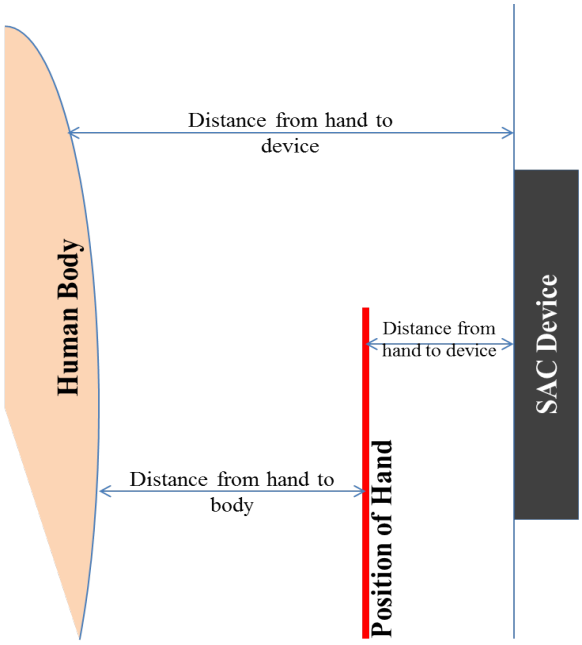


Figure 6.3: Distance Computation

have different hand length.

6.2 SAC System Application

Our system has economical and societal benefits for example. Let us consider our system being used in various environment's such as: Military/top secret department, Banks, Immigration services, etc. In the Military/FBI/CIA departments there are very valuable top-secret data; a breach in such places means a disaster (Economically/Socially). With the help of our system we can differentiate between officials and non-officials or fraud people from entering into secure area. When considering banks the public trusts the security of the bank, and deposits all their hard earned assets into the bank. The security in few banks is so minimal that anyone could enter into the secure part of the bank. As all the employees have just an ID card to enter into the secure part of the bank. Anyone with this ID card can enter as the system only recognizes only the existence of the card but not the user. With the

behavioral feature in our system we can match the user to their ID to avoid unauthorized personals to enter the secure area.

We can also see that our system has a potential in immigration service as well. In the airport, people when entering into the country have to go through immigration check. Here public is scanned for finger print and then checked for background and then they are authorized to enter the country. This process takes time, as there are a lot of people flying in and out of country these days. As the people and flights increase, the waiting time in the security check area is increased. If we setup our system in such places we can reduce the waiting time for innocent public trying to enter the country with a right purpose.

Chapter 7

Conclusion

In this thesis we proposed a novel, scalable security system that avoids the many limitations of the state of the art security systems and act as a basic building block for the future generation security systems. The security system we proposed in this thesis, called SAC system, is adaptive, incorporates intelligent features, and provides enhanced security. In the experimental evaluation, the SAC system showed very good performance just with basic primary level hardware and it provide reliable security with minimal user interaction. A distinct feature of this system is that it implements behavioral learning so that the system can maintain the uptodate information about the users. We believe that the behavioral learning of our system can be improved by including many more primary level sensors in the system, which eventually leads our system to be the best among the security system proposals till date.

We left with many interesting directions for future work. Firstly, our work can be complimented by adding many more pattern sensors to capture the behavioral data of the users efficiently. Secondly, we can have just one sensor at the primary level. One such example of such kind of sensor is the blooming Microsoft kinect sensor. Finally, the scalability of the system can be evaluated thoroughly by installing N-SAC devices to enable multiple access points so that multiple users can try to access to the system concurrently.

Bibliography

[1] Winda Astuti and Syazilawati Mohamed. Intelligent voice-based door access control system using adaptive-network-based fuzzy inference systems (anfis) for building security, 2007.

[2] Alexander De Luca, Katja Hertzschuch, and Heinrich Hussmann. Colorpin: securing pin entry through indirect input. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 1103–1106, New York, NY, USA, 2010. ACM.

[3] Gumstix. `http://www.gumstix.net/wiki/index.php`.

[4] Robotics Recearch Lab. DynamicPIN: A novel approach towards secure atm authentication, 2011.

[5] MaxBotix. `http://www.maxbotix.com/tutorials.htm`.

[6] M. Popa, A.S. Popa, and M. Marcu. A distributed smart card based access control system. In *Intelligent Systems and Informatics (SISY), 2010 8th International Symposium on*, pages 341 –346, sept. 2010.

[7] Junfeng Qian, Shiwei Ma, Zhonghua Hao, and Yujie Shen. Face detection and recognition method based on skin color and depth information. In *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on*, pages 345 –348, april 2011.

[8] Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. It's no secret. measuring the security and reliability of authentication via "secret” questions. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pages 375–390, Washington, DC, USA, 2009. IEEE Computer Society.

[9] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy. Visualizing keyboard pattern passwords. In *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, pages 69 –73, oct. 2009.

[10] Yigang Zhang, Qiong Li, Xinguang Zou, Kecheng Hao, and Xiamu Niu. The design of fingerprint vault based ic card access control system. In *Proceedings of the 5th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications*, pages 172–175, Stevens Point, Wisconsin, USA, 2006. World Scientific and Engineering Academy and Society (WSEAS).

Appendix: Hardware

Gumstix

Gumstix [3] are computers with a motherboard which resemble a stick of gum in size. Even though they are small they have processing speed ranging from 200 to 600MHz. At this speed one can install a Linux OS on the gumstix without any difficulty. Due to the small size they don't have a HD drive as in normal computer, instead it uses flash memory to store data. The available flash memory at present is 4, 8, 16, 32 MBs. Based on the choice of CPU, RAM, storage space, and expansion capabilities there are three motherboard available: Verdex, Connex, and Basix. The one that we used for our implementation is the Verdex. There are a lot of extension available for the verdex, general purpose input/output (GPIO), additional serial ports, Compact Flash cards, USB connectivity, BlueTooth, Ethernet, Robotics Microcontrollers, and Wi-Fi.

Gumstix is an AVR architecture based chips which by itself are called embedded architecture. Due to the small size of gumstix there are no onboard compilers on it for compiling programs. We need to compile the programs on a normal PC and then transfer them on to the gumstix. Since the gumstix and the PC have different architecture, we need to cross compile the program. To do the cross compiling AVR provides a complier avr-gcc, this can be used on any PC to compile gumstix programs. There might be a situation where we need to install the OS again. This process also needs special attention, the Linux image must be built on a regular PC. Gumstix provides buildroot method to build the Linux images.

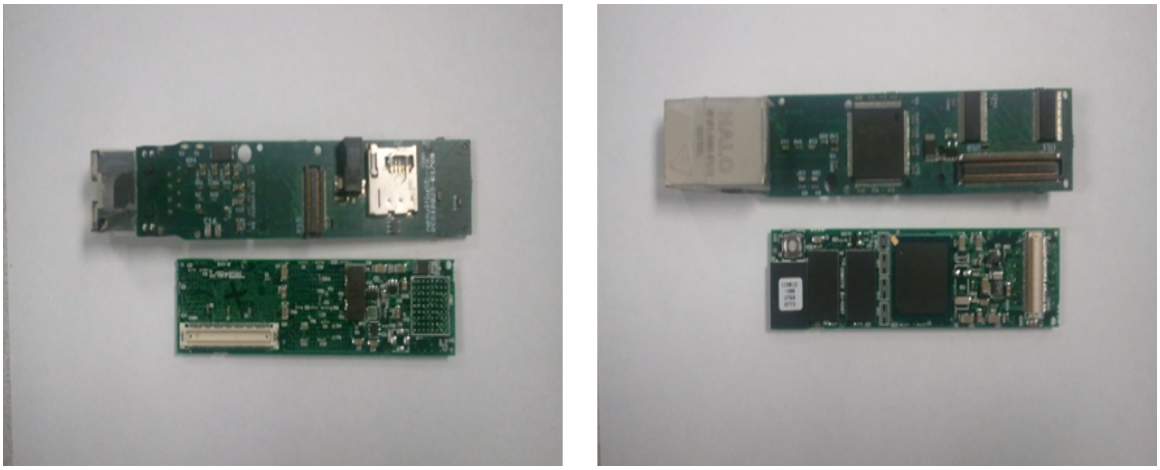


Figure 1: Gumstix Front and Back View

Robostix

Out of the many expansion board that gumstix provides, robostix is one amongst them. Robostix is a microcontroller is also AVR based called ATmega 128. Similar to most of the microcontroller's features robostix has a lot of features as well: ADC, PWM, Ports, UART and Timers. The fact that the robostix has 8 ADC channels with 10bit resolution, it best suits for our implementation since we have sensors that output analog signals. The robostix has various I/O pins that can be used to control external devices like a keypad in our case. Robostix standalone microcontroller can only execute code, because of it has a very slower processor and smaller memory than the Gumstix. In our implementation we need to send sensor values to the Gumstix, in such case we need to connect the Gumstix to the Robostix.

The Robostix is connected to gumstix together serial port also called, STUART (/dev/ttyS2) and UART0. This means that the serial port STUART on Gumstix is connected to the UART0 serial port of Robostix. When connected in this way the Tx port of the Gumstix is connected to the Rx port of the Robostix and the Rx port of the Gumstix connected to the Tx port of Robostix. When the robostix is successfully connected to the Gumstix, robostix now can be programmed by gumstix using the UISP module available on gumstix.

PWM is a commonly used technique for controlling power to inertial electrical devices, made practical by modern electronic power switches. The average value of voltage (and

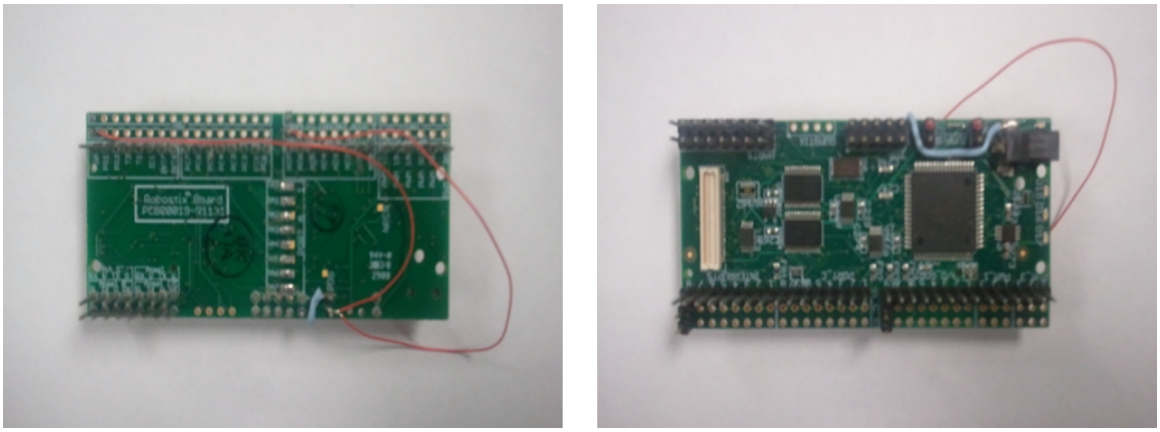


Figure 2: Robostix Front and Back View

current) fed to the load is controlled by turning the switch between supply and load on and off at a fast pace. The longer the switch is on compared to the off periods, the higher the power supplied to the load is. The PWM in Robostix is used for mainly controlling servos which are part of the implementation.

Pin	Label	GPIO	Function	Description
1	PWM 1A	Port B.5	OC1A	Output Compare Match A for Timer 1
2	PWM 1B	Port B.6	OC1B	Output Compare Match B for Timer 1
3	PWM 1C	Port B.7	OC1C or OC2	Output Compare Match C for Timer 1, or Output Compare Match for Timer 2
1	PWM 3A	Port E.3	OC3A or AIN1	Output Compare Match A for Timer 3 or Analog Comparator Negative Input
2	PWM 3B	Port E.4	OC3B or INT4	Output Compare Match B for Timer 3 or External Interrupt 4
3	PWM 3C	Port E.5	OC3C or INT5	Output Compare Match C for Timer 3 or External Interrupt 5

Table 1: Pulse Width Modulation (PWM)

Port C and A is made up of 8 general purpose I/O pins. The row of pins closest to the edge of the board is ground and the middle row of pins is +5v. The pins closest to the middle of the board are described below, Port C is totally dedicated for the keypad. Port A is totally dedicated for the MUX that we used for the weight sensors and sonars.

The ADC pins are connected to a 10-bit analog to digital converter. These pins can also be used as general purpose I/O pins or for connecting a JTAG. The row of pins closest to

the edge of the board is analog ground and the middle row of pins is analog +5v (this is controlled by a different voltage regulator than the +5 on the Port C and Interrupts connectors). The pins closest to the middle of the board are described below.

Pin	Label	GPIO
1	PC0	Port C.0
2	PC1	Port C.1
3	PC2	Port C.2
4	PC3	Port C.3
5	PC4	Port C.4
6	PC5	Port C.5
7	PC6	Port C.6
8	PC7	Port C.7

(a) Port C

Pin	Label	GPIO
1	PA0	Port A.0
2	PA1	Port A.1
3	PA2	Port A.2
4	PA3	Port A.3
5	PA4	Port A.4
6	PA5	Port A.5
7	PA6	Port A.6
8	PA7	Port A.7

(b) Port A

Pin	Label	GPIO	JTAG
1	AD0	Port F.0	
2	AD1	Port F.1	
3	AD2	Port F.2	
4	AD3	Port F.3	
5	AD4	Port F.4	TCK
6	AD5	Port F.5	TMS
7	AD6	Port F.6	TDO
8	AD7	Port F.7	TDI

(c) ADC

Table 2: Ports on Robostix

In the bottom left corner is the 2x8 UARTs connector. UART-0 and UART-1 are the two serial ports available from the ATMega128. UART-0 is used for communication between Robostix and the Gumstix for controlling all the functions of the devices on the interface board. UART-1 is shared between the LCD screen and RFID reader.

Function	Pin	Pin	Function
STUART RxD (GPIO 46)	1	2	Gnd
+5	3	4	robostix UART-0 TxD (Port E.1)
STUART TxD (GPIO 47)	5	6	+5
Gnd	7	8	robostix UART-0 RxD (Port E.0)
robostix UART-1 RxD (Port D.2)	9	10	Gnd
+5	11	12	I2C SDA (Port D.1) labelled TX
robostix UART-1 TxD (Port D.3)	13	14	+5
Gnd	15	16	I2C SCL (Port D.0) labelled RX

Table 3: UART

Sonar

Maxbotix make a wide range of sonars based on the range. We used LV-MaxSonar EZ0 [5] which can operate with 2.5V - 5.5V. At this operating voltage the device can provide very short to long-range detection and ranging, with very good resolution. The LV-MaxSonar EZ0 can detect objects in a range between 0 to 6.45 meters and provides sonar range information from 6-inches out to 254-inches with 1-inch resolution. Objects from 0-inches to 6-inches range as 6-inches. The interface output formats included are pulse width output, analog voltage output, and serial digital output.

Figure 3: Sonar [5]

LV-MaxSonar-EZ0 Pin Out

1. GND Return for the DC power supply GND (Vcc) must be ripple and noise free for best operation.

2. 5V-Vcc : Operates on 2.5V - 5.5V. Recommended current capability of 3mA for 5V, and 2mA for 3V.

3. TX : When the BW is open or held low, the TX output delivers asynchronous serial with an RS232 format, except voltages are 0-Vcc. The output is an ASCII capital R, followed by three ASCII character digits representing the range in inches up to a

maximum of 255, followed by a carriage return (ASCII 13). The baud rate is 9600, 8 bits, no parity, with one stop bit. Although the voltage of 0-Vcc is outside the RS232 standard, most RS232 devices have sufficient margin to read 0-Vcc serial data. If standard voltage level RS232 is desired, invert, and connect an RS232 converter such as a MAX232. When BW pin is held high the TX output sends a single pulse, suitable for low noise chaining. (no serial data).

4. RX : This pin is internally pulled high. The EZ0 will continually measure range and output if RX data is left unconnected or held high. If held low the EZ0 will stop ranging. Bring high for 20uS or more to command a range reading.

5. AN : Outputs analog voltage with a scaling factor of (Vcc/512) per inch. A supply of 5V yields 9.8mV/in. and 3.3V yields 6.4mV/in. The output is buffered and corresponds to the most recent range data.

6. PW : This pin outputs a pulse width representation of range. The distance can be calculated using the scale factor of 147uS per inch.

7. BW : Leave open or hold low for serial output on the TX output. When BW pin is held high the TX output sends a pulse (instead of serial data), suitable for low noise chaining.

We had to connect the all the sonars in a daisy chain fashion, because at first when we connected the sonars in a round fashion without interconnecting them. There was a lot of interference caused between sonars. To avoid interference we had to connect them in a chain, so that only one sonar could send and receive independently.

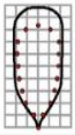
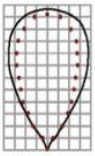
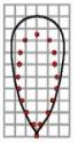
LV-MaxSonar®-EZ beam patterns	EZ0™	EZ1™	EZ2™	EZ3™	EZ4™
Detection pattern to a 1/8 inch diameter dowel.					
Detection pattern to a 1/4 inch diameter dowel.					
Detection pattern to a 1 inch diameter dowel.					
Detection pattern to a 3 1/4 inch diameter dowel. -5V •3.3V V+ supply voltage. (Distances overlaid on a 1 foot grid.)					

Table 4: Beam Width [5]

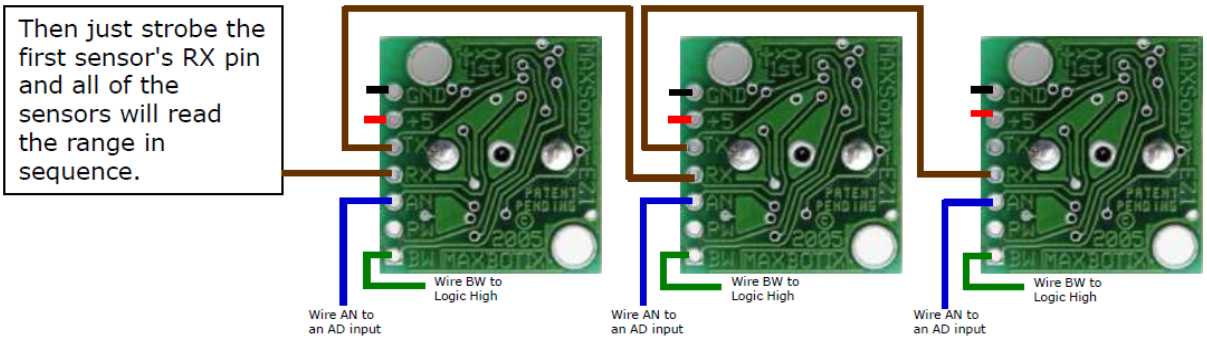


Figure 4: Daisy Chain [5]

Load Cell

Load cell these days are used in many application, from research to industrial use. In present days load cells are in wind towers, suspension and even in weight scale. Apart from the application of load cell there are different types of load cells. Over the past years there are a vast number of developments have been made. Load cell where initially used for strain gauge for measuring direct stress.

The weight sensors that we use for our implementation are load cells, and we calculate measure the stress on the cells. The load cell gives a change in resistance when weight is

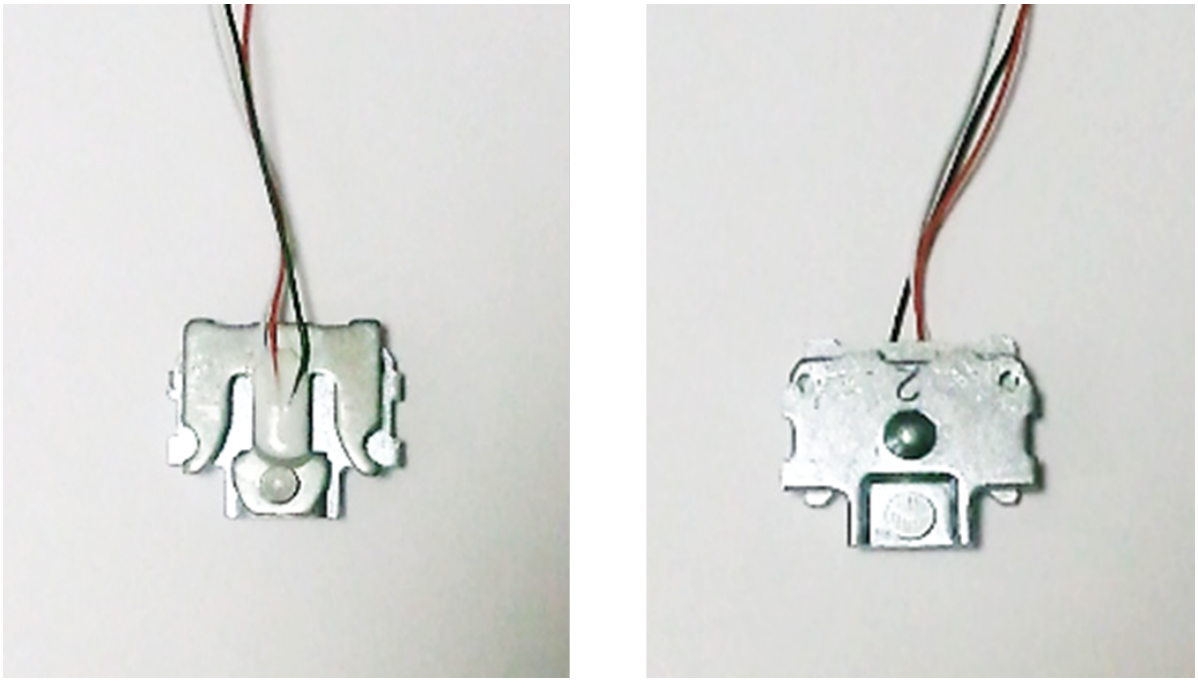


Figure 5: Load Cell

applied on it. When a voltage is applied across the cell, then a change in resistance will cause a small change in voltage at the output. This voltage is too small for a ADC, if we have to feed the voltage to ADC then the output voltage must be amplified using an amplifier.

Vita

Lohit Penubaku was born in India in the year 1983. He did his schooling in Bangalore, India, He graduated from Pre-University in year 2001. Later he joined Nitte Meenakshi Institute of Technology from which he graduated in 2005 with a bachelor's degree in electronics and communication engineering. In 2007 he enrolled into master's program at Louisiana State University in electrical engineering. He has graduated with his first master's degree in engineering science and will be graduating with his second master's in electrical engineering on August 2011.