ADVANCED LEARNING MECHANISM FOR SMART ACCESS CONTROL SYSTEM (SAC SYSTEM)

Master's Project

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 System Science

in

The Department of Computer Science

by
Karthik Nagabandi
B.Tech(C.S), S.R.M University, Chennai, India, June 2010
December, 2011

Acknowledgements

I would like to graciously acknowledge the support of many people that made the completion of this work possible. I would like to thank first my advisor Dr. S.S. Iyengar for his knowledge, understanding, help and patience. I also want to thank Dr. Jianhua Chen and Dr. Konstantin Busch for serving in my committee.

I would like to thank JongHoon Kim without whom this project would not have been a success. I thank him for serving as a mentor, friend and brother in absence of my advisor. I am greatly indebted to him. I would also like to thank Lohit Penbaku, who guided me throughout the project.

Finally, I would like to thank my family for their moral support, who have been a source of strength throughout this work.

Table of Contents

List of Tables

List of Figures

Abstract

Security is the major concern in the society. The resources must be safely protected and in order to protect the resources, proper control must be provided to access the resources. Different methods have been proposed to provide secure access to the legitimate users like traditional lock/key, pin access, smart cards and biometric techniques such as voice recognition, face recognition and many others. The access control systems map the resources to the appropriate users and prevent any kind of loss.

The SAC system is a security system, which is used to provide secure access to the legitimate users by recording the users daily activities and using those activity patterns for providing adaptive security. Analysis of the collected data is performed, where the system carefully chooses users for additional layer of authentication procedure and isolates the legitimate users. The SAC control system also includes the concept of dynamic non-physical key, which uses individual users memory and brainpower to generate and update his security key dynamically. This helps in changing the key regularly with time and making the key more secure and preventing inappropriate users from securing access to the system.

Now that the SAC system is ready to provide secure access to the system, the performance is the major characteristic to be considered. The performance mainly depends on reducing genuine user rejections and bad user acceptance. The faster the system recognizes the user in all situations the better is the system. This project mainly deals with the learning mechanism for the system to adapt and learn the behaviors of the users. The learning mechanism allows the system to select the best match, make system faster, and provide most secure access.

The learning mechanism this project mainly deals with uses a set of valid secure user access; the system performs the respective learning from these valid users and learns to adapt to deviant situations to be more user friendly, secure and accurate. From the final result obtained, the system also corrects the wrong entry by updating the respective weights.

The goal of this project is to make the SAC system more secure and faster making it user friendly. With this learning technique the systems adaptability to different situations increases and making the decision making of the system more reliable.

Chapter 1

Introduction

The safety of property is the top priority of many organizations. Many organizations are working on providing secure access to their resources in order to prevent any kind of loss to their organization. Providing special privileges to their employees can prevent this loss. Access control is a mechanism, which is used to control or protect both the resources and the personnel. One of the most important techniques to implement this security is door security. Various mechanisms have been developed to provide secure access to the doors. 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 etc. and various other biometric techniques.

Biometric techniques have been useful in providing secure access to the resources. These methods are not individually prefect to provide optimal security. These methods are most of the time not user friendly and are not convenient to most of the users. Therefore, the SAC system has been used, which support adaptability features and provide minimum layer of authentication for the innocent users and making it difficult to inappropriate users to pass though the security system.

The SAC system observes and records the daily activities of the users and uses those activity patterns for providing security. From the analysis of the data, the system selectively chooses certain users for additional layer of security and isolates those individuals who pass the scrutiny. Due to this adaptive feature, the SAC system not only minimizes delays and provides more convenience to the users but also enhances the security measure, at the same time. The SAC systems also uses the novel idea of dynamic non-physical key, which makes use of the users memory and brain power to generate and update his security key dynamically so that the key keeps changing with time with out the need of additional devices.

Chapter 2

Background

Security has been major concern in these days. With lot happening around the world, proper security must be provided for accessing. Different methods have been proposed to provide secure access to legitimate users like Voice recognition system, face recognition system, using 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 proved to be helpful in many aspects, but there are some situations where these techniques were easily breached and failed to provide security.

2.1 Access Control Mechanisms

2.1.1 Physical Key

2.1.1.1 Smart Cards

The use of smart cards is the most general secure access technique used by many organizations. Reference 1 describes the latest use of the smart card access system, which uses the Internet as a central control system. The main objective of this paper 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 smart card, which has the users unique identity of the user. This proposed system does not consider the situation of stolen, duplicated, forgotten, lost or impersonated with accuracy. This is very important aspect to be considered since theft is a frequent and easy way to gain access to a privileged room.

Learning: 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.

2.1.2 Biometric

2.1.2.1 Voice Recognition

The research on security access control systems led to the improvement of voice recognition technique. Reference 2 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 is the best characteristics and best 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 on 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 very time consuming and general users do not prefer spending too much time on verifying themselves. The researchers do not mention about the external noise. 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.

Learning: 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.

2.1.2.2 Fingerprints

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 paper aims at overcoming the traditional problems of mechanical locks, such as key lost and personnel transfer. Reference 3 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 do 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.

2.1.2.3 Facial Detection

Facial detection is an important technique in providing access to the room. Reference 4 provides a facial detection technique, which is used to check the genuine users. Junfeng et al.[4] suggests technique, which overcomes the general 2D face recognition technique, which fails 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 ad 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 where the user may frequently find difficulty in accessing the system.

2.1.3 Behavior

The intelligent access control system based on user behavior [1] states that biometrical sensors are sometimes harmful and likely to cause abuse [2,3]. 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 [4]. The final sub-module used Local Outlier Detection for detection of deviant entries [5,6,7]. 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. The attributes, which have the standard deviation close to the average standard deviation, 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

Cons: - Can be made complex - Costly, uses various equipment's for security

Learning: 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.

2.2 Non-Physical

2.2.1 PIN

De Luca et al. [5] proposed ColorPIN, an authentication mechanism that uses indirect input to provide security enhanced PIN entry, and showed that it is notably secure than StaticPIN 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 to a 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 the illegitimate users difficult to 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. [6] 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 used to collect the data, which were used in pattern categorization. This project also checks weather 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 Questions

This method is yet another technique used now a days for security to a user. This method generally generates a security question if the user forgets his password. This can be seen any of the web mail account. How ever many test were conducted to test the reliability of the system [7]. Stuart Schecher et al. have tested the reliability on number of users and the acquaintances. The test included asking security questions to participants and asked their acquaintance to guess the answer. This test resulted in 17

As suggested in the survey [7], this is not reliable as the illegitimate users can guess the answer to the security question of the user, if he knows him. Makin it a unreliable method to provide security.

2.3 Learning Methods

Learning methods in artificial neural networks refers to the changes made to the system based on the external and internal information that flows through the system. The weights are adjusted in order to make the system adapt to the change to the input values. The learning methods generally generate complex inter-relationship with the inputs and outputs to find a particular pattern.

In this project we propose a neural network, which trains the system based on the inputs given. We try to make the system adapt to different postures of the users and recognize the genuine user more accurately. Once the recognition is done we try to make system learn about the users and the changes in the pattern. Based upon the result, we try to tune the system so that it learns adjusting.

2.3.1 Decision Tree Mechanism

A decision tree is a tree in which each non-leaf node has associated with it an attribute (feature), each leaf node has associated with it a classification (+ or -), and each arc has associated with it one of the possible values of the attribute at the node where the arc is directed from

The decision trees have a significant ability to explain the decision even after the classification is made. The trees represent the global properties of the user.

One learning method, which has been implemented in access control mechanisms, is the decision tree mechanism. J48 algorithm is used with the help of WEKA tool, which is the java implementation of Quinlan's algorithm. J48 algorithm is generally used for classification, which is also called statistical classifier. J48 algorithm constructs a decision tree from a set of training data. The training data consists of classified examples. At each node the algorithm chooses one attribute that splits the samples into subsets. The node with the highest normalized information gain is chosen to make decisions.

Classification of various users has been done using the Weka toolkit. Weka is a collection of various machine-learning algorithms for implementing different data mining tasks. Weka is provided with various tools for pre-processing of data, classification, regression, clustering, association rules and visualization. This software can also be used in developing new machine learning algorithms.

Initially this system used average learning method, to authorize users, which is found to be less accurate and does not easily adapt to the new conditions.

Chapter 3

State of the Art

3.1 Behavior Profiling Technique for Access Control System

3.1.1 Intelligent Access Control Systems Based on Users Behavior

The intelligent access control system based on user behavior [1] states that biometrical sensors are sometimes harmful and likely to cause abuse [2,3]. 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 [4]. The final sub-module used Local Outlier Detection for detection of deviant entries [5,6,7]. 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. The attributes, which have the standard deviation close to the average standard deviation, 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 percentage of irregular entries and produced false alarm in 6 percentage of regular entries.

Cons: - Can be made complex - Costly, uses various equipment's for security.

3.1.2 Intelligent Entry Control System

The Intelligent Entry Control [8] system is similar to the system [1]. The difference comes in accessing and collecting the data. This system uses Time and Space database. Every event that is collected by the sensors is stored in the Time and Space database. The event collector is used to gather required information whenever there are events like identity card access, fingerprint recognition, door opening and closing etc. For every sequence of events the event collector generates two signals. The first signal passes through the TCP/IP communication channel, which is used by the intelligent system to retrieve all the data from the database. This event is called the clocked event.

The second signal passes through the message queue to the video controller. The video controller reads the pre-buffered videos and collects images from the camera. Then joins the pre-buffered video sequence with the collected images and save it to the database.

This model proposes different rules for recognize the action of the person. The expert rules are used in this model, where the rules are not learnt from the behavior but are defined by the user from a set of pre-defined generic rules. The intelligent system then reads the data from the database and calls the four threads for each module. When all four threads exit, the main program combines the results from these modules and displays the result, which may be OK, Warning or Alarm.

Cond: 1. Complex, since involves more number of modules ; Databases are volatile.

Chapter 4

System Architecture

4.1 SAC 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.

4.2 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 hardware based on the requirements and functionality for the device. They can be categorized as follows:

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 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.

4.3.1 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.

4.3.2 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.

4.3.3 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.

4.4 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 of 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.

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 SAC Architecture Based System 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.

4.5 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 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.

4.6 Neural Network Design for SAC System

Artificial Neural Network or simply Neural Network is a mathematical model of consisting of three layers namely Input layer, Hidden layer and output layer. Neural network is an adaptive system which adjusts or changes its own structure based upon the external factors. This phase of adjusting generally takes place in a phase called learning phase. They are generally used to find a pattern in the given data and learn the general behavior of the input data.

The simplest form of neural network is the single layer network where in a 'n' input neuron is connected to hidden layers with a final one output neuron. He figure below gives the Multi-Layer Perceptron rule wherein there is more than a single output. An MLP is a network of neurons.

4.6.1 Simple Neural Network

The neural network used in this project, learns from the pattern presented to the system regularly. The system is already presented with some training data, so that whenever a new pattern of the same user comes in, the system can recognize the user. The system also uses the concept of back propagation algorithm, which is used in this system to adjust weights and make the system adaptable to the new changes taking place with the input values given to the system.

The back propagation algorithm allows the errors to be propagated backwards from the outer nodes to the inner nodes. So technically speaking, back propagation is used to calculate the gradient of the error of the network's modifiable weights.

The neural network is trained recursively with different set of hidden values and weights from input to hidden layer and weights from hidden to output until the closest value of the desired output is reached. The weights from the final epoch are stored in the database, which when applied to the test sample gives minimal error.

This system consists of a set of expected values for the sensor values in the system. The input values at the time of login are then compared to the expected values already stored in the database. There is an acceptance range present for the input sensor values for each individual user. The input patterns, which are based on the sensor values returned from the system, are stored initially in the database. This can be categorized as training data.

From the block diagram below, the input sensor values form the input layer; the black box along with the decision making for the correct range of input values form the hidden layer; the access provided to the users is the output layer for the system. Different approaches have been tried to be implemented to get the best neural network and get more accurate and faster results. This project serves as the foundation for the new SAC learning algorithms, which can be enhanced further by adding more constraints on the input data.

The block diagram below shows the general overview of the system. The input values, which are the sensor values are given to the black box. The recognition and learning are done in the black box. The black box then checks for the genuine user and trains the system as well. If the black box does not recognize the input of the specific user then it is forwarded to the second layer, where it requests PIN. The PIN used in this project is the Dynamic PIN, which changes with every login based upon logic. If the user enters the correct PIN, the system is then trained to accept the user with those respective sensor values.

4.6.2 Black Box

The basic block diagram for the black box is shown below:

The above block diagram gives the inner perspective of the black box, where the responsibility of this layer is to find whether the input sensor values are in the given range or not. The weights are adjusted respectively depending upon the expected input and the new data from the respective users.

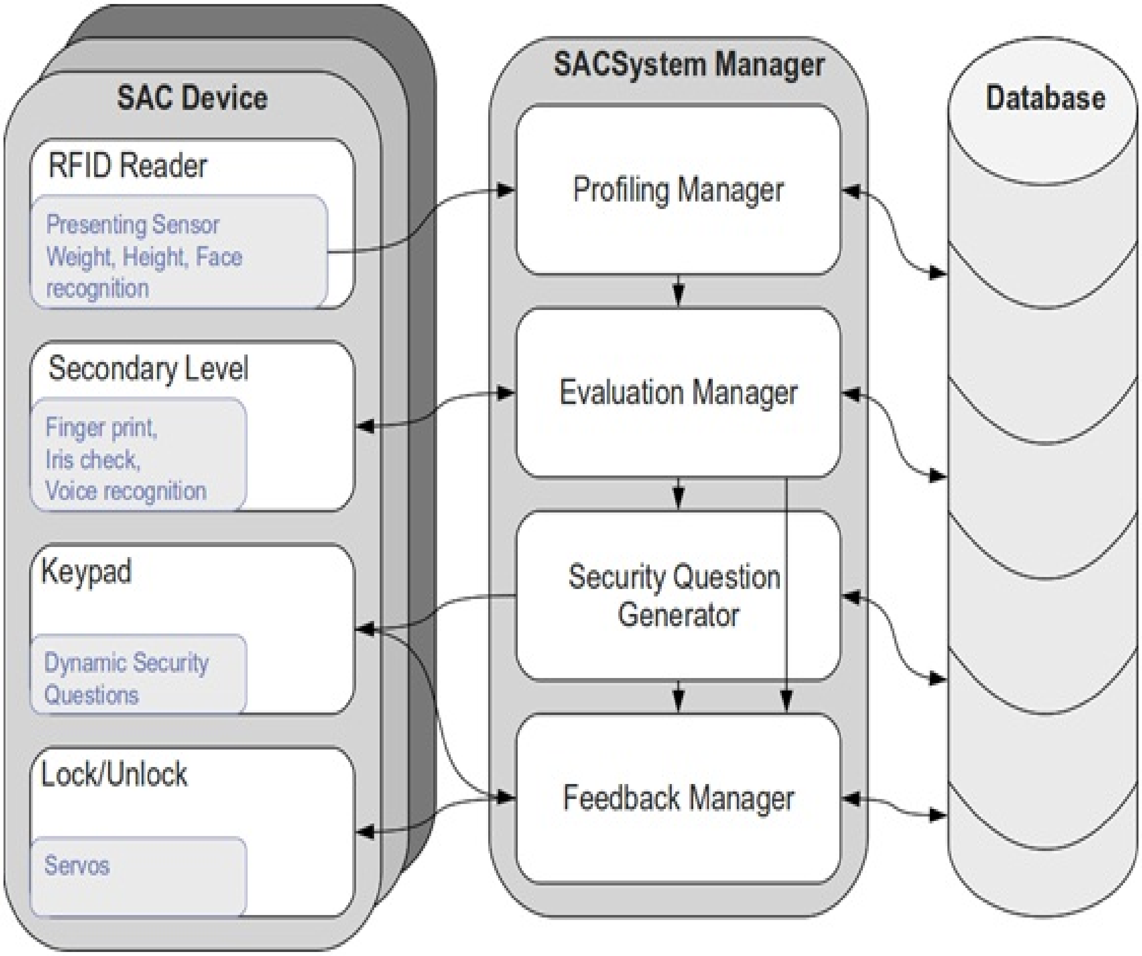
'ExI' in the above block diagram refers to the Expected Input for the respective sensors for a particular user. These are initially stored in the database. When the users enters for the first time the system asks for the DPIN and then compares it with the expected input stored initially in the database. Eventually, the system does not ask for the DPIN and rather recognizes the user with his routine postures (provided he provides a valid ID). This learning makes the system more user-friendly and accurate. Whenever the system doubts the user, it requests for the DPIN and if the user is genuine the system adjusts the weights so that the next time the user logs in with the same posture, he gains access without request for the DPIN.

Once the black box recognizes the given input is in the given range it then counts the number of sensor values of that particular user match within the range. If the number is greater than half of the input values presented, then the system recognizes the user to be legitimate user.

Then using back propagation algorithm the system then adjusts the weights of the input values which resulted to be out of range and adjusts them in order to make the next login faster and recognize the deviant situations.

If the number of input values does not match with at least half of the expected values then the system requests for DPIN and if the user gives the correct DPIN then the system recognizes that particular user to be the legitimate user and then adjusts the weights of the input values which have resulted in rejection of the user, so that next time the same user logins with the same credentials the system does not request DPIN. Thus making the system more user-friendly and accurate.

The generic flow of the system is shown below:



(a) single image title1

Figure 4.1: Oil pipeline inspection robots

Chapter 5

Implementation

From the system architecture, we have seen the general architecture of the SAC system as well as the neural network used for making the system learn.

The block diagram below shows how basic implementation of the SAC system

The SAC System consists of five basic modules:

- **SAC Device** The SAC device consists of Gumstix, Robostix, ADC, Ports, UART at the system end and has RFID reader, keypad, lock/unlock, sonars at the user level.

  The primary level of hardware used in this system is a simple RFID reader, sonars and weight sensors. For user interactive level hardware we used a keypad for the lock and used electromagnetic latch

  Gumstix is a processor which is based on ARM Architecture, also called single -board computers, which has similar potential as a tablet PC. 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.

- **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.

- **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.

- **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.

- **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.

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.

The general presentation scheme used for the SAC System is shown below:

The block diagram show below give the overall implementation of the neural network in the system.

The neural network implementation involves training the system with the varied inputs given to the system for different users. Initially, when the user presents the system with the RFID along with the pattern of sensor values, the system requests DPIN. Eventually as the user continues to access the system, the system learns the new patterns and the request for DPIN gradually decreases unless the system gets a bad input.

From the above block diagram, the input sensor values are given to the neural network, where the input is verified for the acceptance. The input values are compared to the range of acceptance. And if most of the input values belong to range the user is granted access. And through back propagation algorithm, the weights of the inputs which were recognized to be out of range are adjusted. The weights are adjusted in such a manner that, when the user accesses the system eventually these values are also accepted by the system.

If most of the input values are out of range or the system does not recognize the user, it requests for DPIN. If the DPIN matches with the record then the user is granted access and in parallel the weights of the inputs which recognized the inputs to be out of range are adjusted eventually. If the user enters the wrong DPIN the user is not granted access to the system.

A.W block in the above block diagram refers to adjusting weight part of the system. The constraint imposed to the system in this neural network design was to adjust the weights of only those inputs which have resulted in not recognizing the given input in the expected range. This is chosen to be a constant in our neural network. This constant for adjusting can further be adjusted and made dynamic, which is one of our future work to be implemented to the system.

By recursively using different kinds of users with different input variations the system is adjusted to recognize a set of users who access the system regularly. This makes the system more user-friendly and secure as well.

In order to save the user information we have used 'aisac' database which essentially consists of the user information. The neural network stores the user information such as the EID, TID, Sonar values, IR values, Weight Sensor values, valid bit, Expected values for the specific user, Adjust weight values.

Chapter 6

System Evaluation

Below snapshot is the final prototype of the SAC System.

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. This learning process also runs in parallel where the systems learns about the patterns and stores the information in another table depicting the neural network learning of the system. The system constantly updates the database of the user login as well as the learning weights.

The registration table has the basic information of all the users who have access to the lab. We were able to see visually how different users have different presenting patterns. But the system cannot 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.

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.

The snapshots below give the database and the tables used for learning.

Pictures below describe the installation in use and user accessing the system.

Chapter 7

Conclusion

Our system has economical and societal benefits. 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 and 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 cut short the waiting time for innocent public trying to enter the country with a right purpose.

The system can be further be modified, which is left for us for future work. Firstly, our work can be appended by imposing more constraints and changing to make the system more secure. Since the user just presents his pattern and RFID it is also user friendly. Further, the layers in the neural network can be increased in order to get accurate results. The constants which are used in the learning also can be made dynamic, which remain the most important part of our future work. This neural network learning implemented in the system just serves as a foundation. And many other constraints and layers can be complimented to the system, which may make the system complex but makes the system secure, faster and user friendly. We have tried implementing different learning mechanisms compared to our previous results, the proposed neural network had the best results.

Bibliography

[1] Junfeng Qian, Shiwei Ma, Zhonghua Hao, and Yujie Shen.

[2] Yigang zhang, Qiong Lin, Xinguang Zou, Kecheng Hao, and Xiamu Niu. “the design of fingerprint vault based ic card access control system”. In *Proceedings of the 5th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, Madrid, Spain, February 15-17, 2006 (pp172-175).*

Vita

Karthik ...