Contribution of an Embedded and Biometric System in a Replicated Database for Access Control in a Multi-Entry Institution

Bopatriciat Boluma Mangata[1], Eugène Mbuyi Mukendi[2], Jean-Didier Batubenga[3]

[1, 2, 3]Department of Mathematics and Computer Science, University of Kinshasa, Kinshasa, DR Congo
bopatriciat.boluma[at]unikin.ac.cd

Abstract: ***The present work solves the problem of automating access control to the premises in a multi-entry university institution by ruling out possible recurring problems due to falsification of receipts, pretending to be an assistant or a former student, etc. The work is based on the results of a study carried out by a team of experts in the field of access control. On the other hand, there is also the loss or forgetting of the slip for academic fees. To carry out this access control, we have used biometrics based on fingerprints stored in a distributed database that interacts with an on-board system under Arduino, which gives us the possibility of assembling the performance of the programming and the electronics. More precisely, we have programmed electronic systems for the automatic opening of doors without the action of a human being.***

Keywords: Embarked system, biometrics, distributed system, Arduino chart, bases left again data, automation, rigid buzzer, fingerprint, transformations, the orientation of the fields in space

1. Introduction

Security is a major concern in business and commerce through access to information to prevent access by unscrupulous people. In this context, a new technique of access control has appeared: access control by biometric systems. These systems are used both for physical access control (eye, face, etc.) and logical access control (password, smart card, etc.).

To carry out this access control based on fingerprints captured by fingerprint sensors, we are going to use an embedded system under Arduino which gives us the possibility of assembling the performance of programming and electronics. More precisely, we are going to program electronic systems for the automatic opening of doors without the action of a human being. In addition, we are going to arrange the biometric data in each site, making use of the distributed database.

1.1 Problematic

Nowadays, it is certainly difficult for any student present in this university environment to ignore the real problems that arise, as far as student access control is concerned. All the more so as these problems are caused either by certain anti-values that we deplore, such as the exchange of slips, or by certain students in class posing as assistants, former students, administrative staff, etc., or by the fact that they have been given access to the university.

1.2 Hypothesis

That is why, in order to get around these problems, another means of security has been developed which allows the use, not of information that an individual possesses or knows, but of (own) information intrinsic to each person. This new way of identifying individuals is biometrics.

This is why, in this work we will design a new distributed and embedded system for automatic access control to premises based on fingerprints, to put an end to the problems found in the current access control system which is done manually. We want to automate the academic fee control system within a university institution with its students before they access the university site.

To achieve this, we are going to create a distributed system for the availability of biometric data, which interacts with an embedded system for the automation of the opening and closing of doors. This new system will be subdivided into two sub-systems:

a) Enrolment: the sub-system will be able to register the student with his/her registration number, surname, post surname, first name, gender, fingerprint, promotion, faculty, payment status (which may be first instalment, second instalment or all).
b) Identification :
   - Before accessing the university site, the student is expected to provide his or her fingerprint to a fingerprint reader;
   - Once the imprint provided is correct with the current payment settlement then the system opens the door, otherwise the door remains closed.

1.3 Objectives

Throughout this work we will see the importance of biometrics, both embedded and distributed systems in the field of control. All the more so as our new system will allow a better management of access control by eliminating possible recurring problems due to falsification of receipts, pretending to be an assistant or a former student, loss or forgetfulness of academic fees.

Our approach will achieve the following objectives:

- Set up a distributed system using the distributed database;

- Give mathematical reminders about rigid transformations and the orientation of bodies in space;
- To provide a set of precise mathematical definitions for the study of polyarticulated mechanisms;
- Designing an on-board system under Arduino for automatic door opening;
- Designing a fingerprint-based biometric system for access control.

1.4 Interest of the subject

The interest of such an approach is to provide valuable assistance to the scientific community, by providing them with a powerful tool for controlling access to a multi-entry academic institution.

2. Design and Deployment of the System

2.1 Modelling, design and deployment of the project

To carry out this access control based on fingerprints captured by fingerprint sensors, we are going to use an on-board system under Arduino that gives us the possibility of assembling the performance of programming and electronics. More precisely, we are going to program electronic systems for the automatic opening of doors without the action of a human being. In addition, we are going to arrange the biometric data in each site using the replicated database.

We are going to illustrate our system with some diagrams that will allow us to describe the different facets of the software, such as the relationships between the software components, with the outside world (human or other software), over time, etc.

2.1.1. SYSML, Not a Method

SysML is a graphical modelling language derived from UML. This language goes far beyond the problems of computer science. Like UML, SysML is not a method. The diagrams we have used in our work are:

- The requirements diagram;
- The use case diagram;
- The block definition diagram;
- The internal block diagram.

2.1.2. System modelling with SysML diagrams

To solve our problem, here is how our modeling looks, which is represented by the requirement diagram, the use case diagram, the block definition diagram and the internal block diagram :

2.1.2.1. Requirement diagram

Requirement diagram (SysML notation: req) describes the requirements of the functional specification. A requirement expresses a capability or a constraint to be satisfied by a system. It can express a function to be performed by the system or a condition of technical, physical, safety, reliability, ergonomic, aesthetic performance, etc. The requirements serve to establish a contract between the client and the developers of the future system. Here is the model of the requirements diagram of our system:

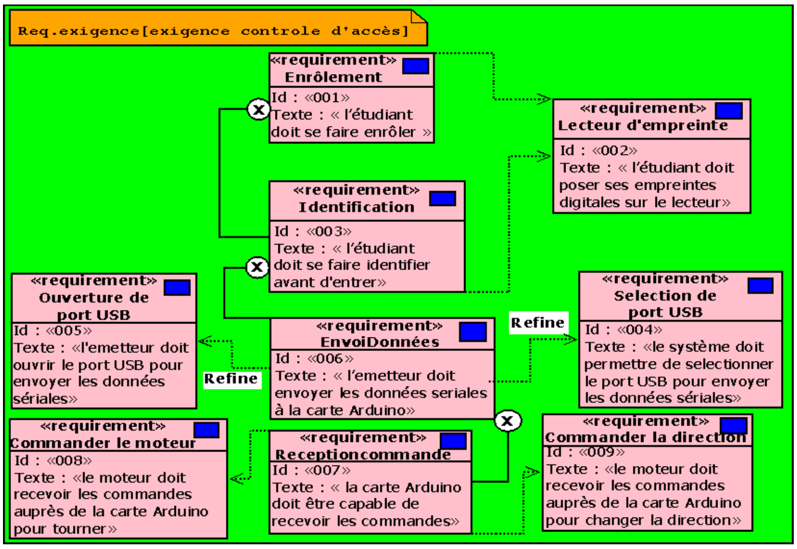

Req.exigence[exigence controle d'accès]
«requirement» Enrôlement
Id : «001»
Texte : « l'étudiant doit se faire enrôler »
«requirement» Lecteur d'empreinte
Id : «002»
Texte : « l'étudiant doit poser ses empreintes digitales sur le lecteur»
«requirement» Identification
Id : «003»
Texte : « l'étudiant doit se faire identifier avant d'entrer»
«requirement» Ouverture de port USB
Id : «005»
Texte : «l'emetteur doit ouvrir le port USB pour envoyer les données sériales»
Refine
«requirement» EnvoiDonnées
Id : «006»
Texte : « l'emetteur doit envoyer les données seriales à la carte Arduino»
Refine
«requirement» Selection de port USB
Id : «004»
Texte : «le système doit permettre de selectionner le port USB pour envoyer les données sériales»
«requirement» Commander le moteur
Id : «008»
Texte : «le moteur doit recevoir les commandes auprès de la carte Arduino pour tourner»
«requirement» Receptioncommande
Id : «007»
Texte : « la carte Arduino doit être capable de recevoir les commandes»
«requirement» Commander la direction
Id : «009»
Texte : «le moteur doit recevoir les commandes auprès de la carte Arduino pour changer la direction»

Figure 1.1: Requirements diagram

2.1.2.2. Diagram of use cases

Use case diagram (SysML notation: uc) shows the functional interactions of the actors and the study system. It precisely delimits the system, describes what the system will do without specifying how (and not what the user will do). It expresses the services (use cases) offered by the system to the users (actors). Here is the model of the use case diagram of our system:

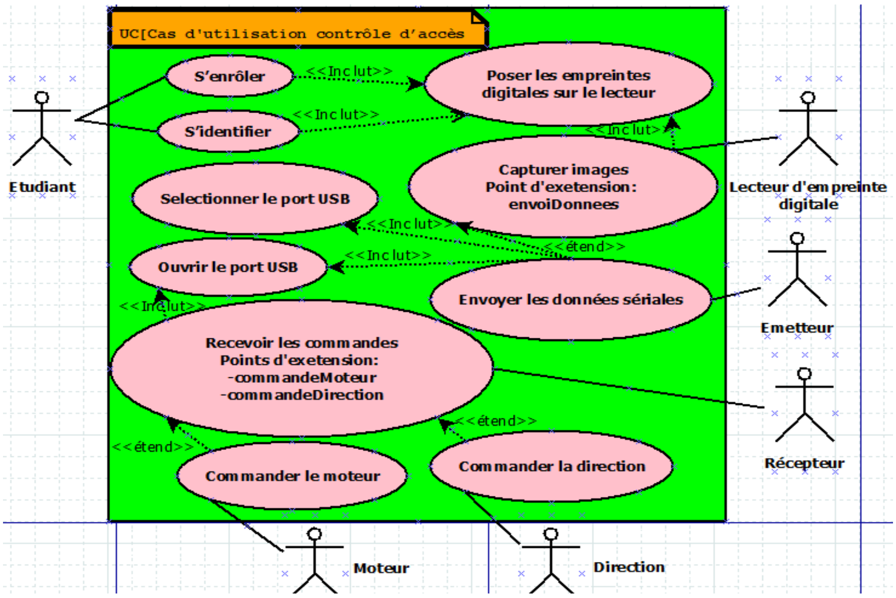

UC[Cas d'utilisation contrôle d'accès
S'enrôler
S'identifier
<<Inclut>>
<<Inclut>>
Poser les empreintes digitales sur le lecteur
<<Inclut>>
Capturer images Point d'exetension: envoiDonnees
Selectionner le port USB
<<Inclut>>
<<étend>>
<<Inclut>>
Ouvrir le port USB
Envoyer les données sériales
<<Inclut>>
Recevoir les commandes Points d'exetension: -commandeMoteur -commandeDirection
<<étend>>
<<étend>>
Commander le moteur
Commander la direction
Etudiant
Lecteur d'empreinte digitale
Emetteur
Récepteur
Moteur
Direction

Figure 1.2: Use case diagram

2.1.2.3. Block definition diagram

Block definition diagram (SysML notation: bdd) shows the system from the component point of view. It answers the question "who contains what". The SysML block ("block") is the basic building block for modelling the structure of a system. This block can represent a complete system, a subsystem or an elementary component.

Here is the model of the block definition diagram of our system:

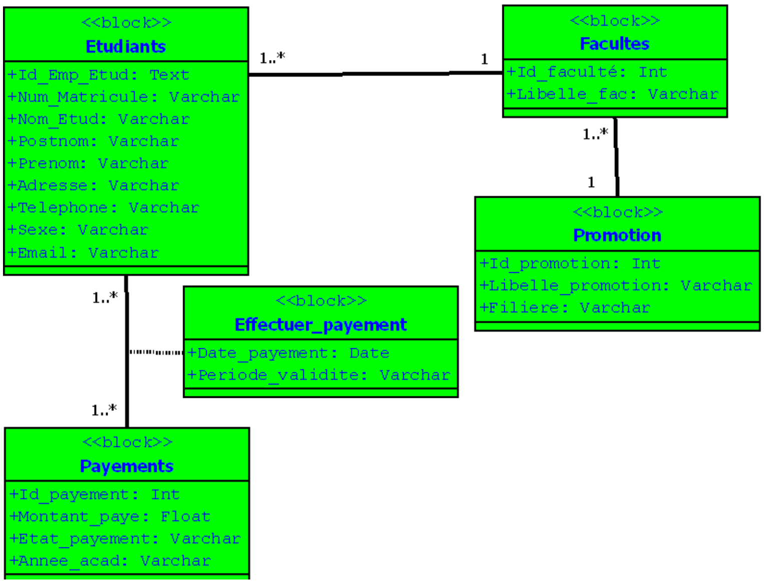


Figure 1.3: Block definition diagram

2.1.2.4. The internal block diagram

Internal Block Diagram (ibd) describes the internal view of a block. It is based on the "bdd". It represents the connection between the elements of a block. The internal block diagram is used to represent the interconnections between blocks. It contains the ports created in the block diagram. The flows of information, energy and matter are clearly shown, flow ports. It also shows the control interfaces, which are standard ports.

Here is the model of the internal block diagram of our system:

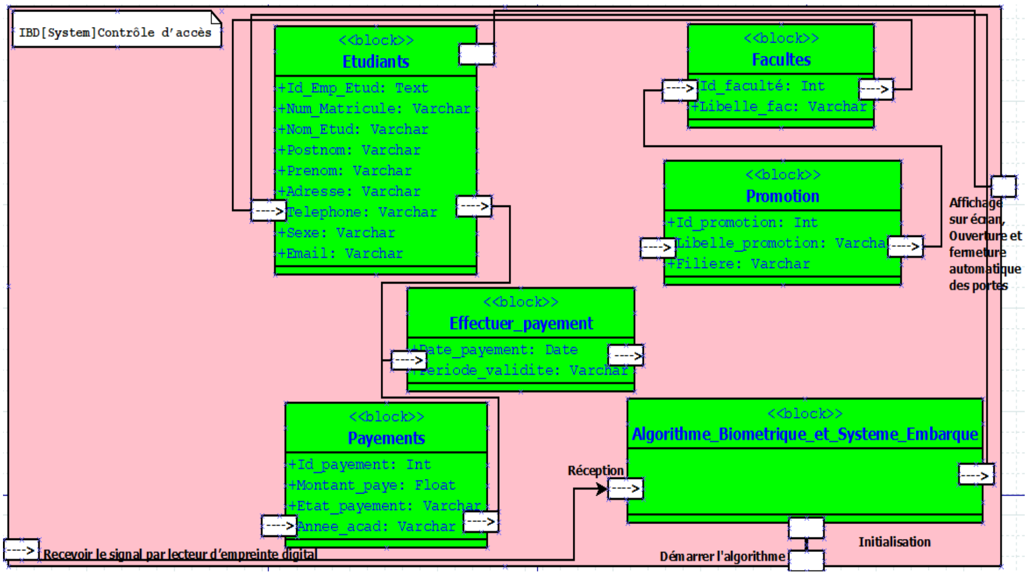


Figure 1.4: The internal block diagram

2.1.3. Data replication model

2.1.3.1. Global Diagram

Our scheme is supposed to be global, it is so by the fact that it no longer concerns a single site so that it is specific only to the latter, but rather all the sites participating in the circulation of information, from which it must be global. In concrete terms, this is the logical data model (LDM) in MERISE or the class diagram in UML. Our global schema is as follows:

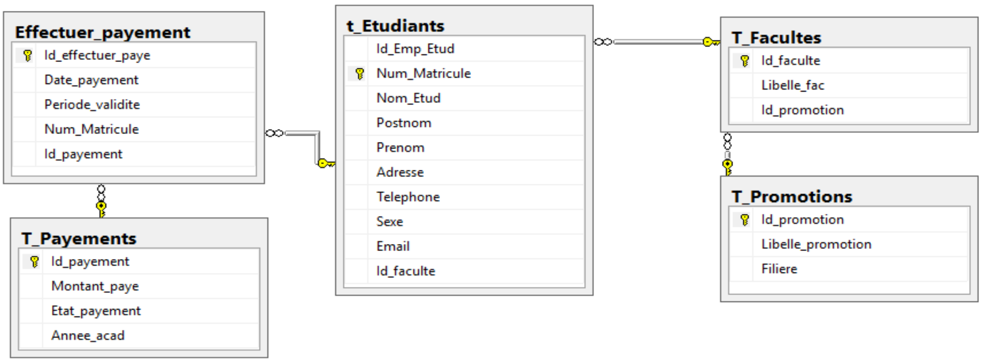


Figure 1.5: Global Diagram

Note: Above is the top-down design, where a distributed database does not yet exist. But if this is the case where databases already exist in different sites; bottom-up design; only common information that could be shared by the different databases needs to be found and a communication mechanism developed.

2.1.3.2 Identification of Sites

We have considered all the offices of the faculty members of UNIKIN, i.e. of each faculty as our sites, but for the time being we will implement only three sites which are :

- SITE I: Office of the Faculty of Sciences' Visiting Professor;
- SITE II: Office of the Faculty Member of the Faculty of Medicine;
- SITE III: Office of the Faculty Visitor of the Faculty of Law.

2.1.3.3. Presentation of the fragmentation plan

Fragmentation is a process of breaking down the overall scheme according to the needs of each site. It precedes allocation, which is the act of allocating these fragments to sites in need.

Fragmentation is therefore based on need, and the need of one site is fed or satisfied by another that holds this information.

In our case, each site will have the same information as the others. Consequently, the fragments of each site will be the tables of our system.

It is important to know that the largest fragment is a table and that the fragmentation of the global scheme is simply a matter of applying the fragmentation on a table or better on each table to either extract part of the data from the table or the whole table. It is therefore not possible to apply it on two (2) tables at the same time even if they are linked.

This way of doing things imposes and poses a problem, for example, when it is a table that mainly keeps only the information of foreign keys and the real or remaining information would be found in other tables, it will therefore be difficult to apply the fragmentation on this table.

Since this problem is also persistent even when developing replication (SQL Server Technology), the first step would be to prepare within a table the desired set of data (i.e., those that one wants to fragment and then allocate), either through trigger techniques, stored procedures, etc., or through the use of the replication system.

For our case, we will create a new virtual table namedV_ETUDIANTSfrom a view that contains all the necessary information from a student:

```
CREATEVIEW V_ETUDIANTS AS
SELECT
[Id_Emp_Etud],[Nom_Etud],[Postnom],[Prenom],[Libelle_fac],
[Libelle_promotion],[Filiere],[Date_payement],[Periode_validite],[Montant_paye], [Etat_payement],[Annee_acad]
FROM [DEA_FABOL].[dbo].[t_Etudiants]
JOIN [DEA_FABOL].[dbo].[T_Facultes] ON
[DEA_FABOL].[dbo].[t_Etudiants].[Id_faculte] =
[DEA_FABOL].[dbo].[T_Facultes].[Id_faculte]
JOIN [DEA_FABOL].[dbo].[T_Promotions] ON
[DEA_FABOL].[dbo].[T_Facultes].[Id_promotion] =
[DEA_FABOL].[dbo].[T_Promotions].[Id_promotion]
JOIN [DEA_FABOL].[dbo].[Effectuer_payement] ON
[DEA_FABOL].[dbo].[t_Etudiants].[Num_Matricule] =
[DEA_FABOL].[dbo].[Effectuer_payement].[Num_Matricule]
JOIN [DEA_FABOL].[dbo].[T_Payements] ON
[DEA_FABOL].[dbo].[Effectuer_payement].[Id_payement]
= [DEA_FABOL].[dbo].[T_Payements].[Id_payement];
```

By way of illustration, here is the most frequently used fragment, which contains all the necessary information of a student who can be distinguished by the faculty to which he belongs.

- **SITE I : Faculty of Sciences**

```
SELECT
[Id_Emp_Etud],[Nom_Etud],[Postnom],[Prenom],[Libelle_fac],[Libelle_promotion],[Filiere],[Date_payement],[Periode_validite],[Montant_paye],[Etat_payement],[Annee_acad]
FROM [DEA_FABOL].[dbo].[ V_ETUDIANTS]
WHERE [DEA_FABOL].[dbo].[
V_ETUDIANTS].[Libelle_fac]='Sciences';
```

- **SITE II : Faculty of Medicine**

```
SELECT
[Id_Emp_Etud],[Nom_Etud],[Postnom],[Prenom],[Libelle_fac],[Libelle_promotion],[Filiere],[Date_payement],[Periode_validite],[Montant_paye],[Etat_payement],[Annee_acad]
FROM [DEA_FABOL].[dbo].[ V_ETUDIANTS]
WHERE [DEA_FABOL].[dbo].[
V_ETUDIANTS].[Libelle_fac]='Medecine';
```

- **SITE III : Faculty of Law**

```
SELECT
[Id_Emp_Etud],[Nom_Etud],[Postnom],[Prenom],[Libelle_fac],[Libelle_promotion],[Filiere],[Date_payement],[Periode_validite],[Montant_paye],[Etat_payement],[Annee_acad]
FROM [DEA_FABOL].[dbo].[ V_ETUDIANTS]
WHERE [DEA_FABOL].[dbo].[
V_ETUDIANTS].[Libelle_fac]='Droit';
```

2.1.3.4. Presentation of the allocation plan

As we said before, each site will have the same information as the others. Therefore, the allocation plan of each site will have all the tables in our system. Here is how our allocation plan looks like:

Faculty of Sciences	Faculty of Medicine	Faculty of Law
t_Etudiants T_Facultes T_Promotions Effectuer_payement T_Payements	t_Etudiants T_Facultes T_Promotions Effectuer_payement T_Payements	t_Etudiants T_Facultes T_Promotions Effectuer_payement T_Payements

2.1.3.5. Presentation of the current layout of each site

In our system, each site will be locally autonomous. Therefore we will have the same schema in our different sites which can be schematised as follows:

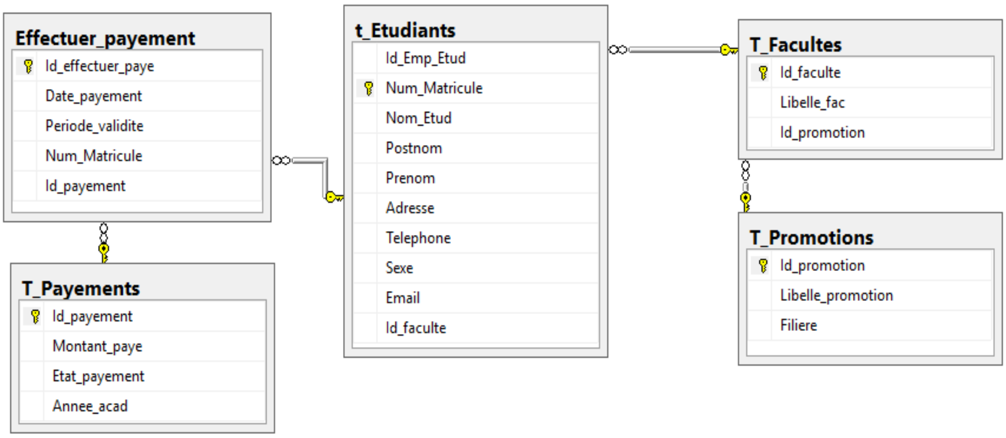


Figure I-6: Current layout of each site

2.2 System Implementation and Architecture

2.2.1. Implementation

In this last part, we are interested in the tools used for the realisation of our application as well as the main interfaces of the application.

2.2.1.1. Choice of hardware and software

Hardware environment

In order to carry out our research project, we have used the following materials:

- Three laptops (LAPTOP) from the HP EliteBook brand.

Here are the characteristics of these machines:

- Mark : HP EliteBook;
- Operating system: Windows 8.1 Professionnel 64 bits;
- Processor : Intel (TM) Core i5 1,70 GHz, ~2,40 GHz;
- RAM Memory capacity : 8 Go;
- Hard disk capacity: 300 Go.

These computers contain a biometric application in C# that allows instructions to be given to the Arduino card via the serial port and a database replicated in three different instances representing our three sites.

- Arduino, is a printed circuit in free material (whose plans are published in free licence) on which there is a microcontroller that can be programmed to analyse and produce electrical signals, in order to carry out very diverse tasks such as charging batteries, home automation (control of domestic appliances - lighting, heating...), controlling a robot, etc. It is a platform based on a simple input/output interface and a development environment using Processing/Wiring technology.

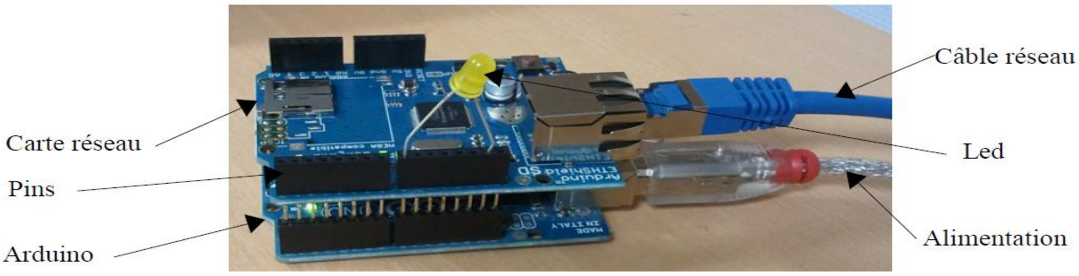


Figure I-7: The Arduino card with its accessories

- TOWER PROTM Micro Servo 9g SG90, a step-by-step motor that will allow us to make the opening and closing movements of the doors;
- Personal Digital, a fingerprint reader, communicating through the USB port.

1) Software architecture

In order to circumvent the problems associated with abusive control of access to the premises, another means of security has been developed which makes it possible to use, not the information that an individual possesses or is known to possess, but (own) information intrinsic to each person. This new way of identifying individuals is biometrics.

The figures below represent the biometric enrolment programme, the biometric identification programme and the Arduino programme respectively.

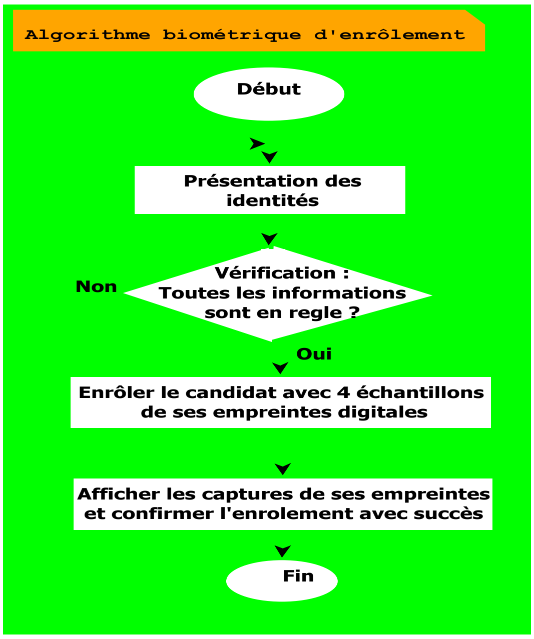

Algorithme biométrique d'enrôlement
Début
Présentation des identités
Non
Vérification :
Toutes les informations sont en regle ?
Oui
Enrôler le candidat avec 4 échantillons de ses empreintes digitales
Afficher les captures de ses empreintes et confirmer l'enrolement avec succès
Fin

Figure I-8: The biometric enrolment programme

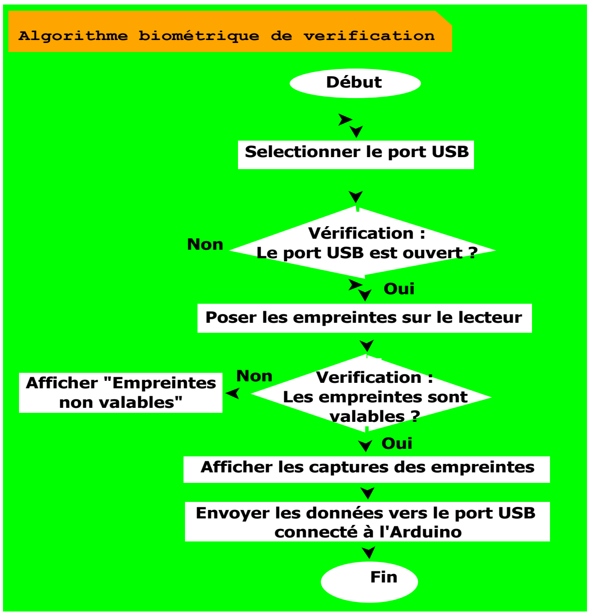

Algorithme biométrique de verification
Début
Selectionner le port USB
Non
Vérification :
Le port USB est ouvert ?
Oui
Poser les empreintes sur le lecteur
Afficher "Empreintes non valables"
Non
Verification :
Les empreintes sont valables ?
Oui
Afficher les captures des empreintes
Envoyer les données vers le port USB connecté à l'Arduino
Fin

Figure I-9: The biometric identification programme

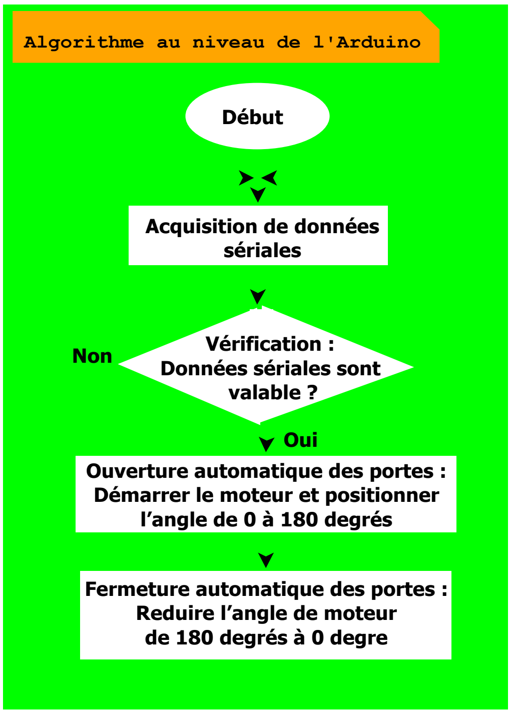

Algorithme au niveau de l'Arduino
Début
Acquisition de données sériales
Non
Vérification : Données sériales sont valable ?
Oui
Ouverture automatique des portes : Démarrer le moteur et positionner l'angle de 0 à 180 degrés
Fermeture automatique des portes : Reduire l'angle de moteur de 180 degrés à 0 degre

Figure V-10: The Arduino door opening and closing programme

2.2.2.2. Hardware architecture of the system

The material architecture of the project is as follows:

- Personal Digital, a fingerprint reader, communicating through the USB port;
- A computer, containing a biometric application in C# that allows instructions to be given to the Arduino card via the serial port and a database replicated in three different instances representing our three sites.
- The Arduino card, which is programmed to analyse and generate electrical signals, in order to carry out automatic door opening and closing tasks (access control).
- TOWER PROTM Micro Servo 9g SG90, a stepper motor that will allow us to make the opening and closing movements of the doors.

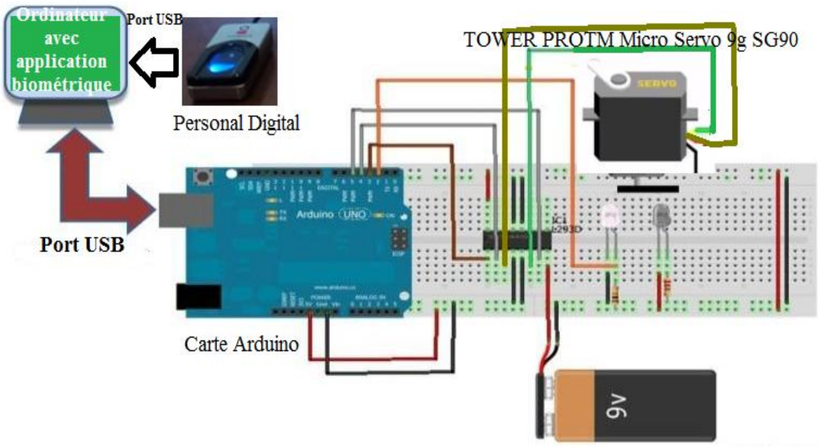

Ordinateur avec application biométrique
Port USB
Personal Digital
TOWER PROTM Micro Servo 9g SG90
SERVO
Port USB
Arduino UNO
Carte Arduino
9v

Figure I-11: Hardware architecture of the system

2.4 Results obtained

Here is a representation of some of the graphical interfaces of our application:

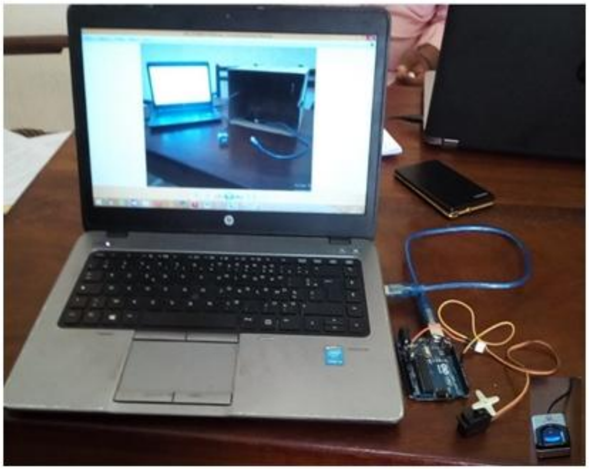


Figure I-12: The material tools of our project

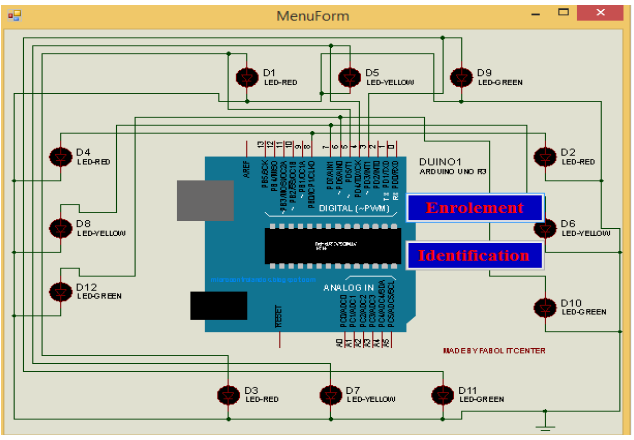
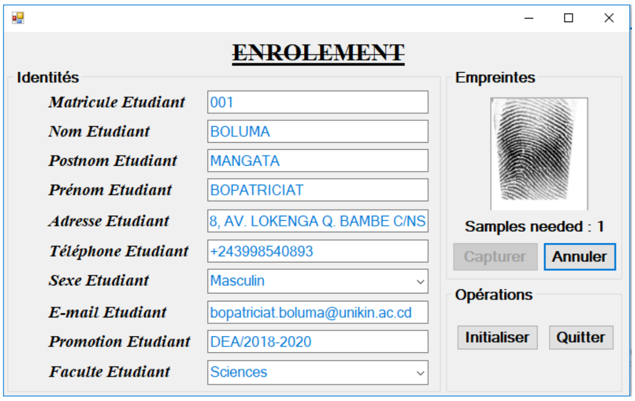


Figure I-13: The application main menu window



ENROLEMENT

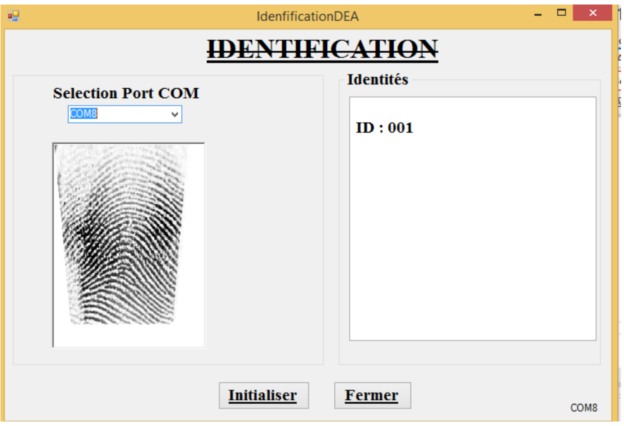
Identités

Matricule Etudiant	001
Nom Etudiant	BOLUMA
Postnom Etudiant	MANGATA
Prénom Etudiant	BOPATRICIAT
Adresse Etudiant	8, AV. LOKENGA Q. BAMBE C/NS
Téléphone Etudiant	+243998540893
Sexe Etudiant	Masculin
E-mail Etudiant	bopatriciat.boluma@unikin.ac.cd
Promotion Etudiant	DEA/2018-2020
Faculte Etudiant	Sciences

Empreintes

Samples needed : 1

Figure I-14: The enrolment window



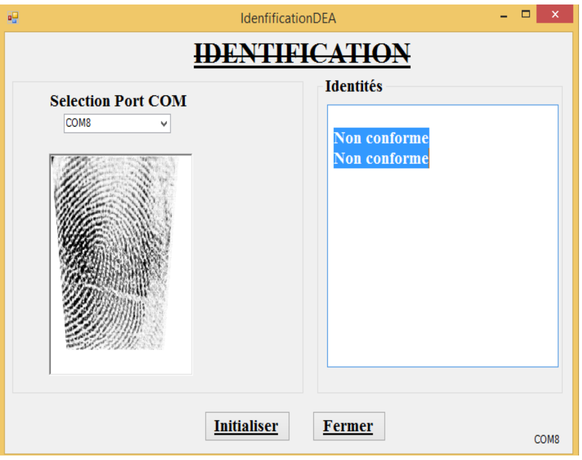
IDENTIFICATION

Selection Port COM: COM8

Identités

ID : 001

Figure I-15: The identification window with a valid fingerprint



IDENTIFICATION

Selection Port COM: COM8

Identités

Non conforme
Non conforme

Figure I-16: Identification window with an invalid fingerprint

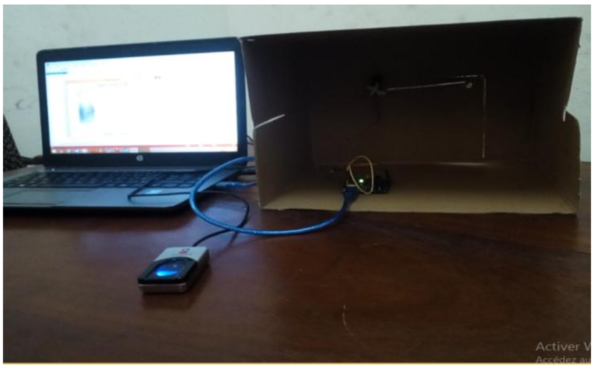


Figure I-17: The project hardware setup window

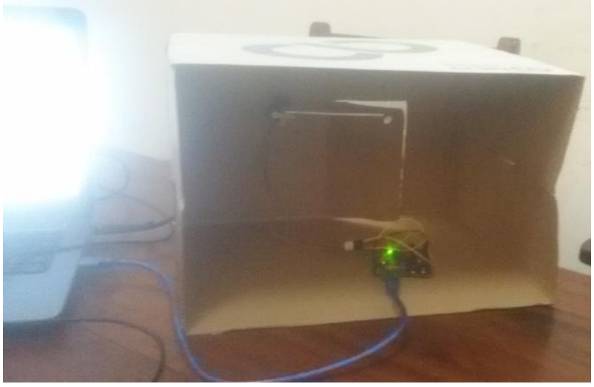


Figure I-18: The test window for opening and closing the door

2.5 System performance

As we said before, the main disadvantage of biometrics is that it does not allow 100% secure authentication, since the measurements are based on physical properties, which can change over time (age, accident, injury, etc.).

A system will be functional when its T.F.R. is low. A system will be safe when its R.F.T. is low. The goal will be to minimize both of these values.
The research tries to limit this EER in order to obtain simultaneously acceptable F.F.R. and F.R.T.

However, on a sample of one hundred individuals consisting of forty women and sixty men, the performance of our system expressed as a percentage is summarised in the table and figure below:

	Staff	Rates FR	Rates FA	Rates ER	System performance
Men	60	2	1	3	57
Women	40	1	1	2	38
Total	100	3	2	5	95

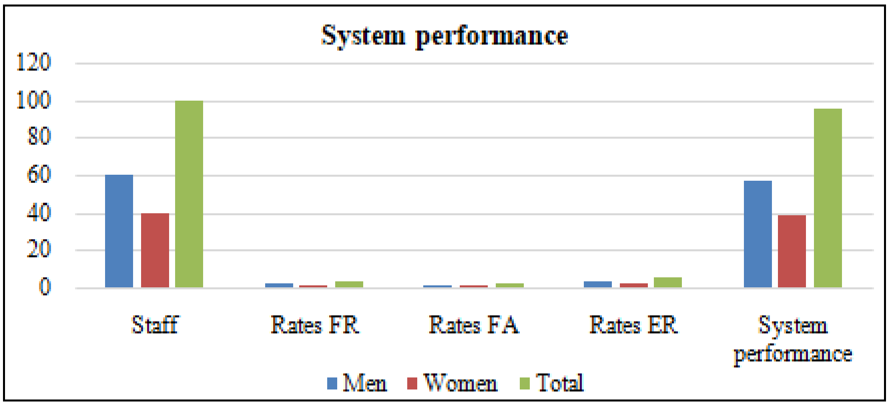


Figure V-19: The performance of our system on a sample of one hundred individuals

In terms of the success rate of the monomodal identification (fingerprint) we have just achieved, we can say that the results obtained are all the more satisfactory since the performance is 95%.

All the tests carried out allow us to conclude that we can take advantage of the merging of several modalities to increase the performance of the identification system because the identification performance of multimodal systems (merging of characteristics or merging of scores) can be applied to give even better results.

3. Conclusion

Here we are at the end of our work, which consisted in designing and deploying a distributed and embedded biometrics-based system for the automation of access control to premises secured by fingerprints, finally putting an end to the problems of abusive access control to premises in a multi-entry institution.

We applied our approach in a multi-entry university institution, namely the University of Kinshasa (UNIKIN).
In order to get around the problems of abusive control of access to the premises, an alternative means of security has been developed that allows the use, not of information that an individual possesses or knows, but of (own) information that is intrinsic to each person. This new way of identifying individuals is biometrics.

Based on this, we have realised a distributed system based on a replicated database using symmetrical technology with synchronous updates, considering all the offices of the Faculty Members of UNIKIN, i.e. of each faculty as our sites, but for technical reasons we have implemented only three sites which are : SITE I (Faculty of Sciences), SITE II (Faculty of Medicine), SITE III (Faculty of Law) finally to ensure the availability of biometric data from fingerprints, which interacts with an embedded system for the automation of door opening and closing. This new system is subdivided into two sub-systems:

a) Enrôlement : le sous-système est capable d'enregistrer les étudiants avec ses identités complètes y compris ses empreintes digitales.
b) Identification (le sous-système est capable de vérifier) :
    - Before accessing the university site, the student is expected to provide his or her fingerprint to a fingerprint reader;
    - Once the imprint provided is correct with the current payment settlement then the system opens the door, otherwise the door remains closed.

As a result, we have had to develop three programmes which are:

- A biometric enrolment programme, which is able to enrol students with their full identities and fingerprints;
- A biometric identification programme, which is capable of verifying information about the person at the door.
- An Arduino programme, which is a programme for analysing and producing electrical signals, in order to carry out the tasks of automatically opening and closing doors (access control) once the fingerprint provided (signal from the biometric identification programme) is correct, then the system automatically opens the door, otherwise the door will remain closed.

The interest of such an approach is to provide valuable assistance to the scientific community, by providing them with a powerful tool for controlling access to premises in a multi-entry institution.

However, we can confirm that our objectives have been achieved, as out of a sample of one hundred individuals consisting of forty women and sixty men, the performance of our system is satisfactory.

In terms of the success rate of the monomodal identification (fingerprint) we have just achieved, we can say that the results obtained are all the more satisfactory since the performance is 95%.

All the tests carried out allow us to conclude that we can take advantage of the merging of several modalities to increase the performance of the identification system because the performance of the identification of multimodal systems (merging of characteristics or merging of scores) can be applied to give even better results.

Throughout this work, we have developed promising techniques and new ideas that will enable us in the very near future to broaden this research theme and tackle the more specialised problems in the field of embedded systems, multimodal biometric systems, distributed systems and potentially distributed databases with more generic solutions.

References

[1] Richard Grisel et Nacer Abouchi, *Les systèmes embarqués*, introduction, Université de Rouen.

[2] Bernard BAYLE, *Introduction à la Robotique*, Université Louis Pasteur de Strasbourg; IUP Technologies Avancées des Sciences du Vivant, année 2004–2005

[3] Jean-Louis Boimond, *La robotique*, Université Angers

[4] Prithviraj R. Shetti , Ashok G. Mangave, *DC MOTOR SPEED CONTROL WITH FEEDBACK MONITOR BASED ON C# APPLICATION*, IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | PISSN: 2321-7308.

[5] Eugene Mbuyi Mukendi, *Intelligence artificielle Approfondie*, L2 Génie Informatique 2014-2015, Math-Info / UNIKIN.

[6] Virginie MATHIVET, L'Intelligence *Artificielle pour les développeurs, Concepts et implémentations en Java, Eni Edition.*

[7] Eugene Mbuyi Mukendi, *Intelligence Artificielle Approfondie*, DEA 2017-2018, Math-Info / UNIKIN.

[8] Renaud Dumont, *Cryptographie et Sécurité informatique*, Notes de cours provisoires 2009 – 2010, Faculté des Sciences Appliquées, Université de Liège.

[9] Christiane Rousseau et Yvan Saint-Aubin, *Mathématiques et Technologie*, Springer Undergraduate Texts in Mathematics and Technology (SUMAT), 2008

[10] Serge Tahé, Sébastien Lagrange, *TP Mobilité et Domotique*, EI5 AGI 2013/2014.

Author Profile

Assistant at Mathematics and Computer Science department in University of Kinshasa, DR Congo. Bopatriciat.boluma@unikin.ac.cd

Ordinary Professor at Mathematics and Computer Science department in University of Kinshasa, DR Congo.

Professor at Mathematics and Computer Science department in University of Kinshasa, DR Congo. jdbatubenga@gmail.com