Development of Visitor Management System Using Smart Card: UMP Case Study

Noorhuzaimi @ Karimah Bt. Mohd Noor, Junaida Sulaiman, Khor Huei Chen

Fakulti Sistem Komputer & Kejuruteraan Perisian,
Universiti Malaysia Pahang
Karung Berkunci 12, 25000 Kuantan, Pahang.
nhuzaimi@ump.edu.my, junaida@ump.edu.my

Abstract - This paper explains the development of Visitor Information System use Smart Card (VIMS) as a smart card-aware application developed to enhance existing visitor registration and visitor information management activities. VIMS replaces the manual recording of visitor information during visitor registration by using visitor's Malaysia Government Multipurpose Card (MyKad). The technology in VIMS are consist of smart card and client server technology. The VIMS enables capturing new visit record by auto-clock in/out, and assignment of visitor pass. Visitor information and visit records are saved in a centralized database server, which provides for management and manipulation of visitor information through searching and report generating. The benefits of VIMS are enhancing the level of security enforced in premises, providing an organized and better view of visitor records and reducing the time spent on managing visitor information. VIMS can be used at different premises, be it government offices, universities, military bases, police headquarters, as long as the premises practice visitor registration and management activity. Further research will be on implementation of mobile smart card reader with biometric verification capability and notification module for fast notification to employee upon arrival of visitor.

INTRODUCTION

Many organizations have their own ways of managing security in their premises and building. One of the security that they need to emphasize on is the security of visitor entering their premises during normal working days. The amount of visitors in certain organization particularly government bodies which give public services such as Jabatan Pendaftaran Negara and Jabatan Pengangkutan Jalan are enormous and can reach thousand in number per day. Other organization such as public institution sometimes receives quite number of visitors with different intentions. Current practice of enforcing security at the main entrance are by registering and recording visitor information in a logbook. This registration activity have some drawbacks. For example, during guard shift exchange, there is a possibility of misplacement of visitor logbook. In addition to that, visitor information in logbook is exposed to every visitor visiting a premise. It is because any visitor can see other visitor's information while they are writing their details in the logbook. It is common that each individual has different hand writing, thus, hand written records can sometimes be difficult to read and search and may not be fraud free guaranteed. Therefore, an automated system of entering visitor information and keeping them in a secured database is recommended to ensure security at the main entrance of the organization.In this paper, we discuss the development of the visitor management system, which introduces a way of registering visitor using MyKad and storing of visitor information for better manipulation of visitor record. The system was developed to gain better visibility of visitor traffic and visitor access control where having the ability to screen and track visitor contributes to the safety and protection of personnel and property. The case study is based on development of visitor management system in Universiti Malaysia Pahang.

This paper is organized as following : the next section will discuss on technology implemented in VIMS .Then, a discussion on system and software design of VIMS is presented . After that, the implementation and testing of VIMS is explained in the following section which is then followed by discussion on the results and lastly , this paper ends with the conclusion section.

VIMS TECHNOLOGY

Smart card reader technology is used in retrieving visitor information from visitor's MyKad. MyKad is a type of smart card with an embedded ATMEL 64K Electrically Erasable and Programmable Read Only Memory (EEPROM) chip [1]. The chip carries the personal information of the card holder. A total of eight applications have been deployed in MyKad to date and replaces the two most important official documents, namely the self identification card and driving license [1]. The identification card number serves as the secure access key to other applications and systems [1]. MyKad

consists of open non-confidential information, which includes cardholder's original name, identification number, gender, birth date, birth place, citizenship, race, religion, address and photo.

The Personal Computer/ Smart Card (PC/SC) specification has been used as the general architecture for the development of this visitor management system. PC/SC includes the general smart card protocol stacks as shown in Fig. 1. The smart card protocol stacks illustrate all layers found in the communication channel between a smart card-aware application and the corresponding application on the smart card [2].

Fig. 1. PC/SC Architecture

The first layer of the smart card protocol stacks consists of smart card services providers (SPP), which each provides an Application Programming Interface (API) that corresponds closely to the command set supported by a smart card. SPP encapsulates the individual functions of a smart card, independent of the operating system used in the smart card. SPP generates Application Protocol Data Unit (APDU) to convey specific command to a specific smart card. APDUs are conveyed to the second software layer within the smart card protocol stacks called the smart card resource manager. Resource manager recognizes the connected smart card reader and smart card. Resource manager routes the APDUs to the third layer of the smart card protocol stack, which is the device driver. Device driver normalizes the differences between the specific I/O channels used by the smart card reader to enable direct communication between the workstation and smart card reader. The APDUs are then passed to the command processor on the smart card, executed, and the results of the execution are then repacked into a response APDU structure and returned through the smart card protocol stack back to the smart card-aware application. [2]

SYSTEM AND SOFTWARE DESIGN OF VIMS

System Overview

VIMS is divided into two modules, which are Guard Module and Admin Module. Process modeling for VIMS represented using DFD, shows VIMS's hierachically divided business processes linked by data flows. Context DFD as shown in Fig. 2 shows the system overview of VIMS, where it includes the system boundaries, entities that interact with VIMS, and information flow between the entities and VIMS. There are two entities as shown in the context DFD, which are Admin and Guard. These two entities depict the users of VIMS and show data flows between both users and VIMS.

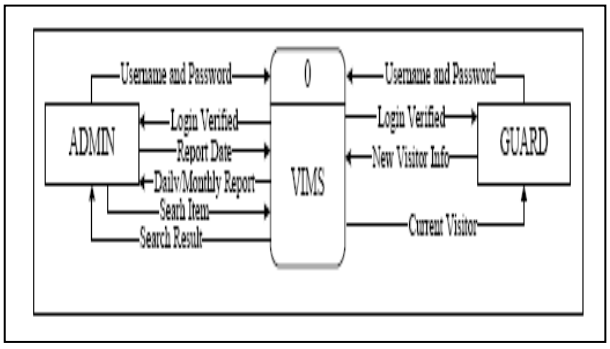

Fig. 2 : VIMS Context Data Flow Diagram

Database Design

For VIMS's conceptual database design, data models are rendered into graphical format using an EERD as shown as Fig. 3. The EERD shows that VIMS consists of five entities, which are Users, Login, VPass, Visitor and Archive. Entity Users is further divided into two types of user, which are Admin and Login.

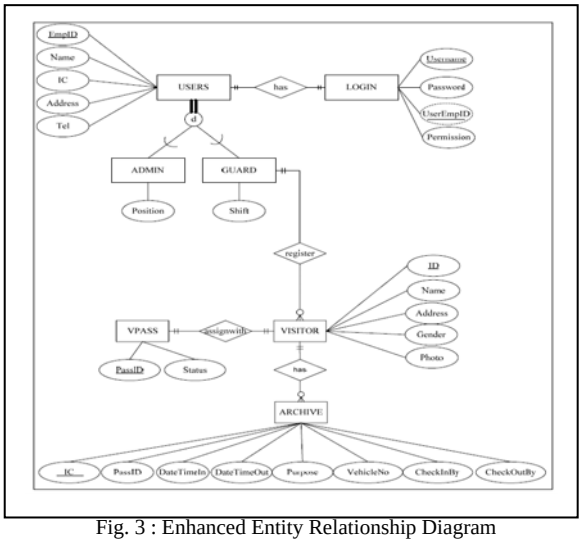

Fig. 3 : Enhanced Entity Relationship Diagram

Interface Design

VIMS consists of two types of interfaces, which one is the interfaces for Admin Module and another is the interfaces for Guard Module. The interface for Admin Module is shown as Fig. 4. The interface for Guard Module is shown as Fig. 5.

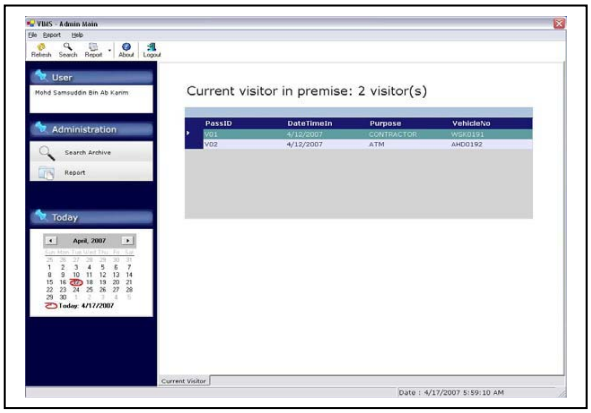

Fig. 4 : Interface for Admin Module

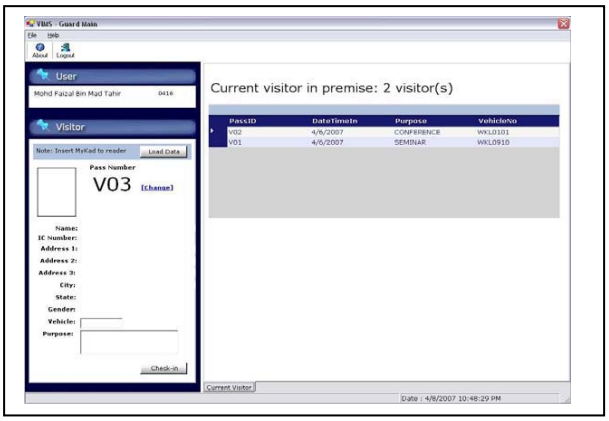

Fig.5 : Interface for Guard Module

IMPLEMENTATION AND TESTING

At system implementation stage, a functional system was developed and tested to ensure the system fulfills business and design requirements. For example, to enable open data to be read from a MyKad, VIMS's source code calls on the functions in the libraries provided in the MyKad Software Development Kit (SDK). A code snippet and process flow on how to the functions in MyKad SDK is called to obtain open data information from MyKad is as shown as Fig. 6.

The SDK used for development of VIMS is the MyKad PC/SC v2 SDK by Iris Corporation Berhad. An USB type smart card reader, Iris SCR21U has been used to provide communication between VIMS with MyKad. Iris SCR21U is a type of fixed terminal smart card reader supported by MyKad PC/SC v2 SDK. It is attached to computer system through an USB port.

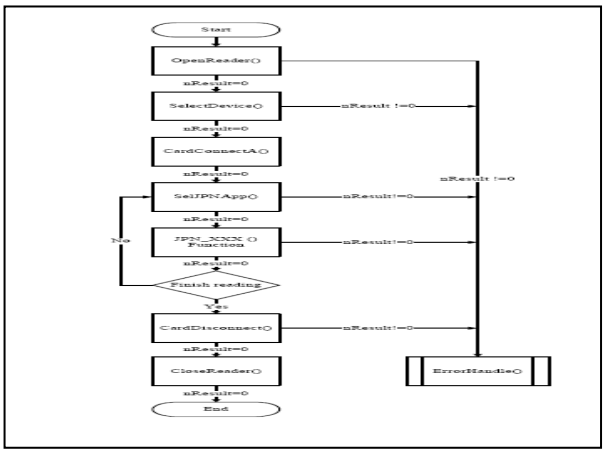

Fig.6 : Mykad SDK Application Programming InterfaceFlow

The testing of VIMS is conducted in a 2-tier client server architecture, where two computers are connected in a local area network. One computer functions as client workstation and another computer functions as the database server. For the unit testing process of VIMS, aspects such as programs code, system interfaces, error handling paths and input/output were considered. Table 1 lists the test cases in VIMS's unit testing.

Table 1 : Test Cases for Unit Testing

Module	Use Case	Description
Admin	Login	Ensuring only authorized users are allowed to login. Ensuring password is not displayed in readable form on screen.
	Print Report	Ensuring report can be printed as shown on interface.
	Search	Ensuring visitor information can be retrieved from database through searching using visitor's name or vehicle registration number.
Guard	Login	Ensuring only authorized users are allowed to login. Ensuring password is not displayed in readable form on screen.
	Register Visitor	Ensuring visitor information is readable from MyKad reader. Ensuring visitor information can be saved into database. Ensuring automated clocking of visitor check-in and check-out time.

RESULTS

VIMS has been successfully developed and tested in the two-tiered client server environment. It consists of two modules; Guard module and Admin module as shown in Fig. 7. The system is capable of:

(i) Retrieving open National Registration Department data from visitor's MyKad.

(ii) Automate assignment of visitor pass based on availability during visitor registration.

(iii) Tracking of who is in premise, purpose, time in, time out and security officer on duty.

(iv) Facilitates searching of visitor credentials and report generating.

(v) Functions in a client-server environment with a centralized record of visitor traffic.

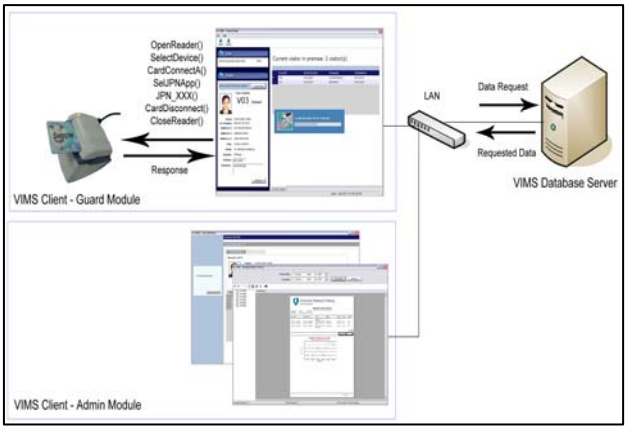

Fig. 7. VIMS configuration diagram

CONCLUSION

With the introduction of VIMS, an organization is able to have an option in increasing the level of security enforced in their premises. VIMS enables free, secured, fast and easy visitor registration. Centralized records gives better management and manipulation of data, through searching and report generation.

VIMS is extensible, where it is able to adopt more functions and futher enhancement that will allow it to provide better functionality and visitor management capability for its user. Among the enhancement identified for VIMS are implementation of mobile smart card reader with biometric identification capability, contactless smart card reader and a notifcation module to notify host within the connected local area network upon arrival of visitor.

Further research includes adding extra security measures by including biometrics function along with existing technology. In addition to that, other module such as visitor notification for visited person is also in consideration for future enhancement.

REFERENCES

[1] National Registration Department, *MyKad Malaysia Multipurpose Smart Card*. 2005. [Internet]. Available from: <http://www.jpn.gov.my/kppk1/Index.htm>

[2] Jurgensen, T. and Guthery, S., *Smart Cards the Developer's Toolkit*. Upper Saddle River, N.J.: Pearson Education, Inc, 2002.