Development of Lumped-Input Access System

Ahmad Yusairi Bani Hashim, Nur Asshafee'i Muhd Zain, Ruzaidi Zamri, Adnan Rachmat Anom Besari
Department of Robotics & Automation, Faculty of Manufacturing Engineering,
Universiti Teknikal Malaysia Melaka, Karung Berkunci 1752, Durian Tunggal, 76109 Melaka, Malaysia
Email: yusairi@utem.edu.my

***Abstract*—Passwords, smart cards, and biometrics that act as inputs are common approaches in security systems design. The operational and functional methodologies of these systems are, however, distinct from one another. There is increasing number of specialists in the field due to widespread use of passwords, smart cards, and biometrics authentication systems. Therefore, the technologies are becoming open secrets. As a result, security systems that apply these technologies are vulnerable to intrusions unless unorthodox methods are fused together to make the systems least exposed. Typical systems design approaches involve estimations on how well they should perform. It is uncommon to model them in an abstract way. Modeling by abstraction, if properly performed can create powerful algorithms that can be difficult to decode. This paper presents abstract formulation style to system design. It shows the formulations of a lumped password-biometrics input; explains how definitions to every components are made, the flow of information, and the execution style.**

***Keywords* — Access system; password; biometrics.**

I. Introduction

A typical security system is the home security. Because it is a system, the block diagram that the system should have is the input-plant-output configuration. In fact, all security systems have this configuration in common. The difference among them is the "plant" block. It is the algorithms that run multiple programs within. They are unique to the individual system that only the designers understand them. In security systems, vulnerability to attacks has always been an issue in the process of designing them. Due to the fact that they are heavily relying on computer programs, computer geniuses might easily hack the codes regardless of the algorithms complexity.

Computerized and networked security systems using multi modal authentication are not new [2], [4]. In fact, it is important to look into the security issues such as the authentication and authorization in information sharing in web services [3]. There are weaknesses of traditional secure access methods such as smart cards and the personal identification number systems; however, it is suggest that biometrics is a promising yet proven approach to efficient authentication and authorization of certain people [1, 5, and 6].

The researchers in [7] suggest combining biometric and state-of-art sensorial technologies to enhance security in wide spectrum of applications. In a more complex situation, researchers in [8] analyze the NATO recommendations in information evaluation for Intelligence. NATO advises procedures that evaluate reliability of the source of the information.

Within this paper, it presents non-definitive formulation of an access system. How this formulation let a lumped password-biometrics input to function in the access system; how definitions to every components are made, the flow of information, and the execution styles are explained.

II. Background

A. General System Representation

Biometrics comes in the form of physiological and habitual. Examples of physiological biometrics include fingerprints, palm prints, the deoxyribonucleic acid, face, and iris. Examples of habitual biometrics are computer keyboard keystroke patterns, hand signatures, voice, and ambulation patterns.

It is proposed that the access system has several inputs (see Fig. 1): the password, fingerprint, smart card, and the face image. The level of access is determined based on these inputs. For the basic level, the input is the password. For intermediate level, the input is lumped with password and fingerprint. Lastly, the advanced level has smart card and face image as the lumped-input.

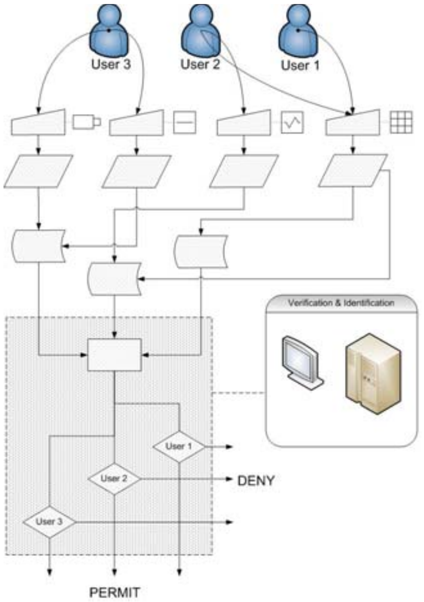

Figure 1. Users 1, 2, 3 have their own level of access. User 1 with a basic security level who shall have access through a password input, whereas users with higher security level shall have access through biometrics and smart card data input.

B. Model

Password—A password is data in a form of series of alphanumeric combination. Let $\mathcal{I}_{\mathrm{P}}$ denotes a password. Therefore, all $\mathcal{I}_{\mathrm{P}}$ represent passwords.

Access card—An access card is a data in a form of embedded information onto the card itself. Let $\mathcal{I}_{\mathrm{C}}$ denotes an access card. Therefore, all $\mathcal{I}_{\mathrm{C}}$ represent smart cards.

Biometrics data—Biometrics data may represent in several forms of traits such as fingerprints and face. Let $\mathcal{I}_{\mathrm{B}}$ denotes biometrics data. Therefore, all $\mathcal{I}_{\mathrm{B}}$ represent biometrics data where additional subscripts denote the type of traits.

User—If a user $\mathcal{U}$ subscribes to the system and attempt to access it, for a given access procedures $\mathcal{U}$ must be scanned.

Agent—An agent is a self-governing algorithm that is designed to seek specific data and transport the grouped data along selected routes within the system. It may perform stopovers at selected locations. Let $\mathcal{A}$ denotes agents. Therefore, each $\mathcal{A}$ executes unique jobs.

Stopover point—At each stopover has predefined functions where A shall have to follow. Let $\mathbb{S}$ denotes stopover point, which is the verification and identification modules. Therefore, $\mathbb{S}$ designates stopover points.

Security level—Let $\mathcal{L}$ denotes security level that determines the type of activation when agents submit the grouped data.

Expression (1) describes the lumped input that consists of data extracted from password, smart card, and biometrics data. In fact, it describes inputs taken through respective input devices from an active user in which the data is brought to $\mathbb{S}$. At $\mathbb{S}$ the data shall be processed and the determination of $\mathcal{L}$ is made. Upon initiation of (1), the system executes access permission or deny to users.

$$\exists\left(\mathcal{I}_P ; \mathcal{I}_C ; \mathcal{I}_B\right) \qquad (1)$$

Suppose there are three regular users 1, 2, and 3 of the access system where each has been assigned to distinct security levels as depicted in Figure 1. That means they only have access to the assigned section. User 1 ($\mathcal{U}_1$) is assigned at the basic security level ($\mathcal{L}_{\mathrm{BSC}}$); user 2 ($\mathcal{U}_2$) at the intermediate security level ($\mathcal{L}_{\mathrm{IMT}}$); and user 3 ($\mathcal{U}_3$) at the advanced security level ($\mathcal{L}_{\mathrm{ADV}}$). So that for the basic security level, the user accesses using a password, the intermediate level by password and fingerprint, the advanced level by smart card and face image. With the conditions of permit (P) or deny (D), following (2) only user 1 can access the system. This also suggests that each user can only access to an assigned section hence (5).

$$\text{PRESENCE } \mathcal{U}_1 \text{; CARRY } \forall \mathcal{I}\left(\mathcal{I}_{\mathrm{P}}\right) \text{ BY } \mathcal{A} \text{ TO } \mathbb{S} \text{ DECIDE at } \mathcal{L}_{\mathrm{BSC}} \rightarrow \mathrm{P} \oplus \mathrm{D}. \qquad (2)$$

$$\text{PRESENCE } \mathcal{U}_2 \text{; CARRY } \forall \mathcal{I}\left(\mathcal{I}_{\mathrm{P}} ; \mathcal{I}_{\mathrm{B,\ fingerprint}}\right) \text{ BY } \mathcal{A} \text{ TO } \mathbb{S} \text{ DECIDE at } \mathcal{L}_{\mathrm{IMT}} \rightarrow \mathrm{P} \oplus \mathrm{D}, \qquad (3)$$

$$\text{PRESENCE } \mathcal{U}_3 \text{; CARRY } \forall \mathcal{I}\left(\mathcal{I}_{\mathrm{C}} ; \mathcal{I}_{\mathrm{B,\ face}}\right) \text{ BY } \mathcal{A} \text{ TO } \mathbb{S} \text{ DECIDE at } \mathcal{L}_{\mathrm{ADV}} \rightarrow \mathrm{P} \oplus \mathrm{D}. \qquad (4)$$

$$PD \equiv P \oplus D \left| \begin{array}{l} (p \oplus d)_{BSC} \neq (p \oplus d)_{IMT} \neq \\ (p \oplus d)_{ADV} ; \mathcal{U}_1 \neq \mathcal{U}_2 \neq \mathcal{U}_3 \end{array} \right. \square \qquad (5)$$

III. Operation

In Table 1, the hardware used is shown with respect to the type of input used. For example, inputting a password would be done using the keyboard. The smart card reader is used to read information from a smart card, and the fingerprint scanner and webcam are used to read biometrics information. Similarly, in Table 2 the software used is shown with respect to the stopover point and the input type. For a password input and a card input; VB.NET is used at the stopover 1 and MS Access at stopover 2. In addition, at stopover 3, special software is used in processing biometrics input. The VeriFinger is used to process fingerprint data, the VeriLook for processing face images.

The testing the of the model was done using the following software and hardware: VB.NET, Microsoft Access, VeriFinger 6.0, VeriLook 3.2, Futronic's FS82 FingerPrint scanner with ISO7816 smart card reader, and a Logitech's webcam. So that from (1), the inputs are acquired from respective hardware listed in Table 1. From (2), the inputs submitted are processed by respective software listed in Table 2. Figure 2 shows the station where the user should manually input the information required in order to access the system. The station has a computer display installed along the webcam, the fingerprint scanner, and the smart card reader on the upper section. It stands close to two meters high.

TABLE I.
INPUT TYPES AND THEIR RESPECTIVE HARDWARE

Input	Hardware
$\Im_P$	Keyboard
$\Im_C$	Smart card reader
$\Im_B$	Fingerprint scanner, webcam

TABLE II.
INPUT TYPES AND THEIR RESPECTIVE SOFTWARE

Input	Software		
	Stopover 1	Stopover 2	Stopover 3
$\Im_P$	VB.NET	MS Access	-
$\Im_C$	VB.NET	MS Access	-
$\Im_B$	VB.NET	VeriFinger, VeriLook	MS Access

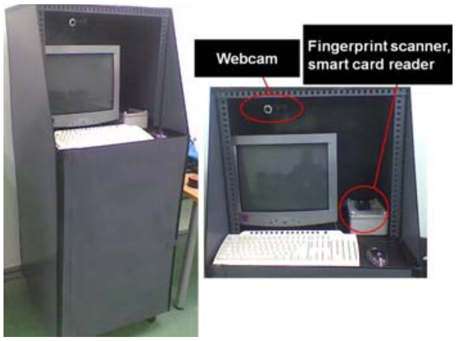

Figure 3. The actual hardware used in the access system consists of a PC, webcam, fingerprint scanner and smart card reader.

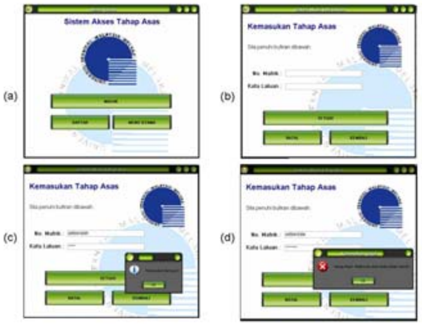

Figure 2. (a) The main graphic interface to gain access to the system at basic level. (b) The interface that allows the user to submit identification and password. (c) The result if entry is confirmed and (d) if the entry is denied.

Upon the initial attempt to access one's account the user would confront a graphic user interface as shown in Figure 3a. This is the basic level interface. The registered user, however, could access the system by clicking on the "*MASUK*" button. When entered the user would be asked for an identification number "*No. Matrik*" and the passphrase "*Kata Laluan*" (see Figure 3b). If an unregistered user would attempt to access the system the output shown in Figure 3d would be displayed saying that the person has no record in the system "*Maaf, maklumat anda tiada dalam rekod*". In fact, this follows (2) with the result "D". Conversely, if a registered user would access the system, the output interface would be shown as in Figure 3c and therefore follows (2) that result in “P”. However, for a new user, the “*DAFTAR*” button should be clicked so that he could register.

The registration process for the basic level is straightforward. First, the user will be asked if he is registering for the basic level (see Fig. 4a). If yes, then the he would key in the appropriate information (see Fig. 4b). If the password section is left unfilled, a message reminding the process would pop-up (see Fig. 4b). A successful registration is shown through a pop-up message (see Fig. 4c) confirms that the user has been registered. Registration for the intermediate and advanced levels is a bit complex. The main interface shown in Fig. 5a allows the prospective user to select the assigned level. If the user is registering for the intermediate level, he will be asked to submit two types of information (see Fig. 5b). One is the password another is the fingerprint (see Fig. 5c). If the user is registering for the advanced level, he will be asked for the face image (see Fig. 5d) and a special card will be produced by the administrator. The registration for the intermediate and advanced levels also follows the specific requirement required by (3) and (4). In (3), the requirement is that the user must possess information in the form of a password and fingerprint data so that the agent compiles them as a packet then submit it to the stopover 2. At this location, the packet would be unzipped and the data would be matched with the registered ones. If the data match then the user would have the “P” result that means the system permits the user to gain access, otherwise he would get the “D” result. Similarly, in (4), the user must have information in the form of face image and a special card so that the agent would bring the packet to the stop over 3. The overall description of the authentication requirement is summarized in (5).

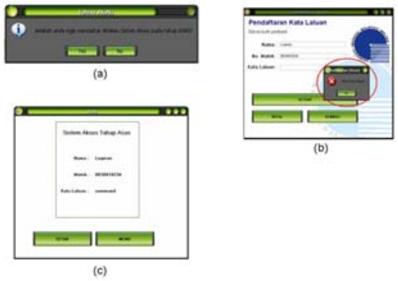

Figure 5. (a) The interface asking if the user do want to register for the basic level. (b) The pop-up that reminds the user to enter a password. (c) The confirmation that the user has been successfully registered.

IV. Conclusion

The codes can be written in any types of programming languages based on (1) to (5). In fact, these formulations are open for modification. While this style of formulation is not a foolproof approach but it offers flexibility in designing system that works in multitude of codes written by different programmers as oppose to flow chart and architectural approaches. It is believed that lumped-input methodology tolerates segregation of users’ accessibility to specified sections. It also obscures users’ combination of keys to access the system from intrusion. In addition, this combination could be made to self-evolve in time-based or event-based so that computer geniuses who mean harm to the system would face difficulty in determining the right key combination.

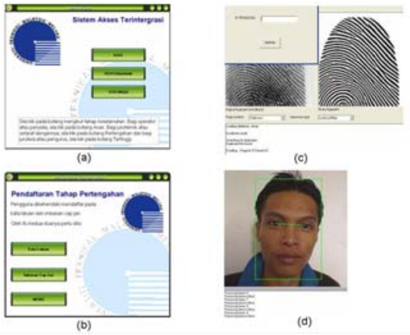

Figure 4. (a) The interface that allows the user to select the assigned security level. (b) The interface for the intermediate level. (c) The fingerprint data and user’s identification. The image capture and authentication.

Acknowledgment

This work would not have been realized without all the equipment and support provided by UTeM and is funded under the Fundamental Research Grant Scheme FRGS/2007/FKP(5)-F0030.

References

[1] A. Jain, R. Bolle, S. Pankati, Biometrics Personal Identification in Networked Society. Boston: Kluwer Academic Publishers, 1999.

[2] A.Y. Bani Hashim, “On Biometric Technology in Security Systems,” Proc. of the International

Conference on Science and Technology (ICSTIE 2006), Dec. 2006.

[3] C.C. Huang, T.L. Tseng, R.R. Gung, H.S. Chang, “An agentbased web services solutions to colloborative product design. Int. J. of Knowledge-based and Intelligent Systems, vol. 9, pp. 63-79, 2005.

[4] D. Desimoz, J. Richiardi, C. Champod, A. Drygajlo, “Multimodal biometrics for identiti documents (MbioID),” Forensic Science International, vol. 167, pp. 154-159, 2007.

[5] J. Ashbourn, Biometrics: Advanced Identity Verification. London: Springer, 2000.

[6] J.D. Jr. Woodward, N.M. Orlans, P.T. Higgins, Biometrics. California: McGraw-Hill/Osborne, 2003.

[7] I.G. Damousis, D. Tzovaras, E. Bekiaris, “Unobtrusive multimodal biometric authentication: The HUMABIO project concept,” EURASIP Journal on Advances in Signal Processing, vol. 2008, Article ID 265767, pp. 11, doi:10.1155/2008/265767, 2008.

[8] J. Besombes, V. Nimier, L. Cholvy, “Information Evaluation in Fusion using Information Correlation,” Proc. of the 12th Int. Conf. on Information Fusion (FUSION ‘09), July 2009.