***IJACSSE** - International Journal ofAdvanced Computer Systems and Software Engineering*
Copyright © Publisher Scientific Academia Network (Scientiaca)
E-ISSN: 2716-5256 online

Biometric Multimodal Security Simulation on Schedule Ii Controlled Drug

Muhammad Amree' Ferdaus Bin Hamdan[a], N.Fuad[b], M.E.Marwan[c]

[a]*Faculty of Electrical and Electronic, Universiti Tun Hussein Onn Malaysia 86400 BatuPahat, Johor, MALAYSIA*
[b]*Computional Signal, Imaging and Intelligence (CSII) Focus Group, Universiti Tun Hussein Onn Malaysia 86400 BatuPahat, Johor, MALAYSIA*
[c]*Kolej Poly-Tech MARA BatuPahat, Sri Gading 83300 BatuPahat, Johor MALAYSIA*

** Corresponding author:*

ARTICLE HISTORY
Received: 7 September 2020
Accepted: 2 October 2020
Published Online: 28 October 2020

KEYWORDS
Multimodal Biometrics
Recognition Tools
Security Product

ABSTRACT

The paper present a multimodal (multi biometrics) security system focusing on the implementation of fingerprint recognition and facial feature recognition to enhance the existing method of security using password or personal identification number (PIN). This project is operated through a personal computer where all the identification for fingerprint and facial feature are done by using specific software. Successful identification will send a signal through a serial communication circuit and open an application. In this project, the final application should be a cupboard that store and secure schedule II controlled drug in hospital. Due to some problem, the final application was replaced by using a light emitting diode (LED) simulation circuit.

1.0 INTRODUCTION

Schedule II controlled drug such as diamorphine, morphine, pethidine are expensively high value and were accepted as analgesic-type drug used in hospitals. This type of drug was illegally abused because of its lack of security level (Tabash, M., &Abuqamar, M. 2018)

The word biometric originated from the Greek roots, *bio* and *metrics* which literary means 'life to measure'. Biometric deals with the identification of individuals based on their biological or behavioural characteristics.Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, etc (Scavia, D. 1995)(Graevenitz, G. A. 2003)

2.1 Problem of Statement

Currently the security rooms that store the Schedule II controlled drug in a hospital only limit the access to the credential user. The individual in-charge is responsible to possess the double-locked key to the room or cabinet. The other alternatives is by the used of numerical keypad or ID card reader to proved the access. (Tabash, M., &Abuqamar, M. 2018)

These methods have possibility to hack since disadvantages of using the manual key and lock that could be lost, stolen, forgotten or misplaced. Numerical keypad problem could be human's memory limitation since the password required for security purpose is a long and complex to ensure a password cannot be guessed. Otherwise, a simple password could be guessed. These methods are far from user-friendly. If the possessions e.g., keys or password fall into the wrong hands, they could abuse the privilegesof the authorized user. Furthermore, the methods cannotdistinguish between the real authorized user and the imposters (Tabash, M., &Abuqamar, M. 2018)(Scavia, D. 1995).

As a result, the biometrics technologies should be considered since it is represent 'what you are' by your physical features or behavioural characteristics. This approach could possibility solve the problems arise.

1.1 Project Objectives

i. To learn the biological characteristics of fingerprint and facial feature.
ii. To learn the implementation of hardware and to combine the hardware and software division into one system.
iii. To study the effect of threshold values in biometric recognition software.
iv. To provide a higher level of controlled drug security system in hospital by combining two biometric characteristic.

2.0 LITERATURE REVIEW

2.1 Threshold Values

The framework holds data on implied and explicit scores for certain user interface objects. Upon user request, the Software accesses the user profile and the associated knowledge preferences files (Shaikh, A. 2020). A value, predefined by the system administrator which is used to establish the degree of correlation between the biometric provided and the stored template that will result in a match (Scavia, D. 1995). (Jain, et al. (2003), reviewed that the purpose of introducing the threshold setting which help to solve the biometric measurements problem that the same individual taken at different times are almost never identical.

2.2 Fingerprint Recognition

(Graevenitz, G. A. 2003) presented the fingerprint identification can be placed into two categories; minutiae-based matching (analyzing the local structure) and global pattern matching (analyzing the global structure). Most of the computer aided fingerprint recognition use the minutiae-based matching. Minutiae points are local ridge characteristics that appear as either a ridge ending or a ridge bifurcation. The uniqueness of a fingerprint can be determined by the pattern of the ridges and the valleys a fingerprint is made of. A complete fingerprint consists of about 100 minutiae points in average. The measured fingerprint area consists in average about 30-60 minutiae points depending on the finger and the sensor area.The use of non-online methods with the facility of individual accounts with their username and passwords does turn out to be one of key positives to gain more customers on daily basis(Soobia Saeed et al.2020).

2.3 Facial Feature Recognition

(Ramzi, et al. (2005), presented a new mechanical platform for camera device which fully automated adjust the camera to eye levels of the persons in front or approaching the system. The system serves as a front end to aid the face recognition and iris recognition systems during enrollment and verification of different people of variable heights. Currently most systems are positioned at fixed height and require subjects to adjust themselves for enrollment. This application which had been demonstrated in United States Immigration VISIT system help the results obtained in iris and facial recognition technologies.

2.4 Dispensary Security System In Hospital

The dispensaries of drug and medicine system in hospital are organized as shown in Figure 2.1 According to (Tabash, M., &Abuqamar, M. 2018), had reviewed that the controlled drug focused on Schedule II Controlled Drug were required to be stored in secure conditions and their use was strictly regulated. These drugs are kept in a difference security room or dispensary security cabinets in hospital. The Misuse of Drug Regulations 2001 places the responsibility for the possession, safe custody and issues of controlled drugs within hospital wards with the senior register nurse in charge of that ward. The senior register nurses responsible to supervise and hold the possession of controlled drug security room or dispensary security cabinets. They can order and receive the controlled drugs as written in prescription. Pharmacists' only responsible supply and checking the controlled drug stocks and registers while doctors sign the drug prescriptions for the clinical use.

Figure 1: Schedule II controlled drug security cabinet.

According to (Tabash, M., &Abuqamar, M. 2018), Schedule II Controlled Drug of the Misuse of Drugs (Safe Custody) Regulations 1973 such as diamorphine, morphine, pethidine had been illegally abused and sold because of their expensive values. These controlled drugs are narcotic type drug were accepted and used in medicine with the classification as analgesic drug which help relieves pain.

2.5 Serial Communication Circuit

Refer to (Mohd Yusof 2006) who proposed serial communication circuit which consists of microcontroller PIC16F84A, MAX232 voltage regulator and RS232 9-pin connection. The programmable PIC expected to control of RS232 transmission and reception through interrupts. The microcontroller sends feedback the received characters back to the terminal window.

3.0 METHODOLOGY

3.1 Project development

This project can be divided into two main parts:-

i. Hardware: The hardware part consists of fingerprint scanner device, web-camera and the serial communication circuit.
ii. Software: The software includes MPLab IDE for the development of microcontroller programming, VeriFinger 4.2 for fingerprint recognition, VeriLook 2.0 for facial feature recognition, Microsoft Visual Basic 6.0 to develop and design the graphical user interface (GUI)

The hardwares and softwares are develop simultaneously and will be combined into one system. Figure 2 shows the project development.

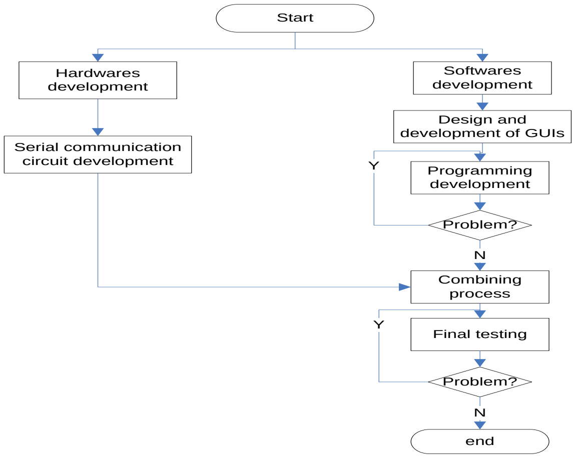


Figure 2: The development process.

3.2 Multimodal Biometric System

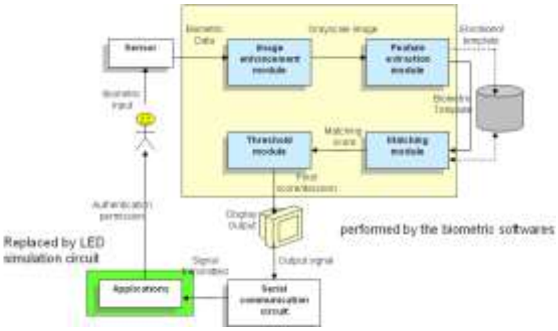


Figure 3: The block diagram.

The project covered is a security system which implements the use biometric technologies. Two biometric characteristic; fingerprint and facial feature will be implemented which recognize and identify the credential user and gives them the access to a target area. To verify the identity of a user by automatically extracting minutiae from his or her biometric image, a biometric recognition algorithm is required. The recognition algorithm is composed of two main technologies: image processing technology that captures the characteristics of the corresponding fingerprint by having the image under-going several stages and matching algorithm technology that authenticates the identity by comparing feature data comprised of minutiae with templates in a database such as discussed in (Jain, A. et al 2003). Image processing implementation generates better recognition process.

These sensors are used to acquire the data needed for recognition and to convert the data into a digital form. The quality of the sensor used has a significant impact on the recognition results. In this project, sensors being used were in form of web-cam for facial recognition and fingerprint scanner for fingerprint recognition.

Database is very important to restore the template information while doing the comparison purpose. Once enrolment occurred, a new template will be produced and restored into database.

Whereas the matching module will prosecute the comparison between template obtained from sensors and the enrolment templates in database. Matching module will generate a matching score after the templates comparison. The matching score generated will be slightly differentiated after one attempt to another.

After that, threshold module will compare the matching score generated with the threshold value sets by the administrator in the biometrics software. After scores being generated, threshold module will determine final result whether user can successfully access into the controlled drug security room. The final result will be displayed at the display screen of the system. An ID represent the identity will appeared if the user passes the recognition procedures mentioned above. Otherwise, the user should repeat the procedure if the access is come to failure.

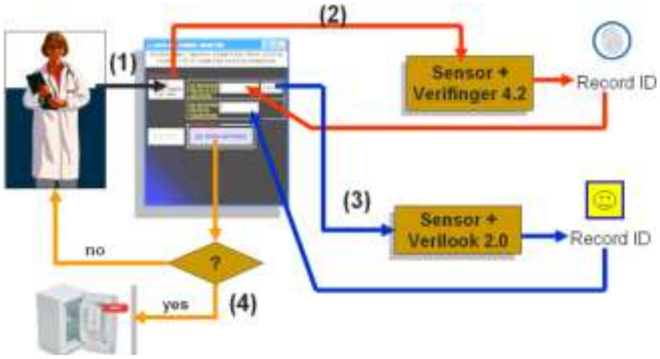


Figure 4: The concept of system.

Figure 4 shows the concept system. The users are require to click the button on the screen that connected to the biometric softwares i.e. VeriFinger 4.2 and VeriLook 2.0. After obtain the record ID that represent the user which provide by the software, then the users are required to enter it into the textbox. The system will check the registered record ID in databases. The access passed if the record IDs were a registered ID.

3.3 Software Implementation

Software	**Function**
MPLab IDE	Implement to design and develop a programming into PIC16F84A microcontroller which is one of the main components in serial communication circuit.
Microsoft Visual Basic 6.0	To design GUI that display the input from the user and the output simulated by the biometric software.

VeriFinger Demo	4.2	To identify user through fingerprint recognition.
VeriLook Demo	2.0	To identify user through the facial feature recognition.

Table 1: The software implementation

3.4 Hardwares

3.4.1 Fingerprint scanner

Fingerprint scanner use as a sensor to scan and to capture the images from fingerprint. DigitalPersonaU.are.U® 4000B was implemented as fingerprint scanner in this project and it is well-acceptable toVeriFinger 4.2 Demo as fingerprint recognition tools. The user simply places their finger on the glowing reader window and the reader quickly and automatically scans the fingerprint.

Figure 5: digitalPersonaU.are.U® 4000B fingerprint scanner.

3.4.2 Web-Camera

Web-cam used as one of the facial recognition tools. Any types or brands of web-cam are acceptable as long as the camera should have minimum resolution of 640x480 pixels. In this project, Logitech™ QuickCam Go was proposed as a web-cam.

Figure 6: Logitech™ QuickCam Go web-cam.

3.4.3 Serial Communication Circuit

The project uses the serial-type communication with the PIC-RS232 interface using the MAX232. Assembly language developed in PIC16F84A In the serial communication, data is transmitted bit-by-bit and the serial port communication requires less connection since it requires three wires for transmit, reception and grounding function.

After several considerations, the real application that is schedule II controlled drug in hospital was replaced by the LED simulation circuit which connected to the system and receive the signal through the serial communication circuit. LED was connected to pin RA1 of a PIC microcontroller. Figure 7 shows the serial communication circuit including the LED.

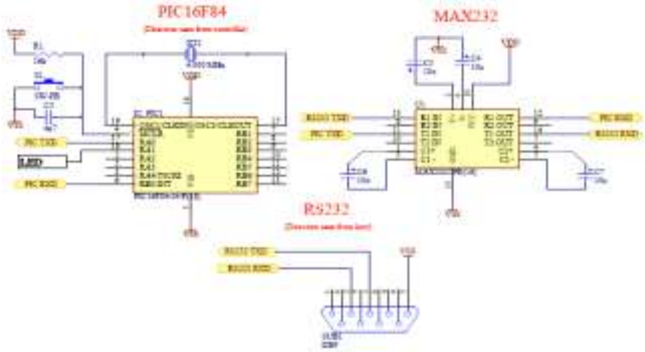


Figure 7: Serial communication circuit.

4.0 RESULTS

4.1 Visual Basic Program

Figure 8 shows the graphical user interface (GUI) that will open and execute the biometric software. A registered credential user will not have a problem from being recognized by biometric software. Successful fingerprint recognition using verifinger will open and execute the next facial recognition. The LED turned on indicate the user had passed all the biometric recognition and able to enter the security room. Figure 8 and figure 9 show the successful recognition of identity using verifinger and verilook will show a record ID. After obtain the record ID that represent the user, then the users are required to enter it into the textbox.

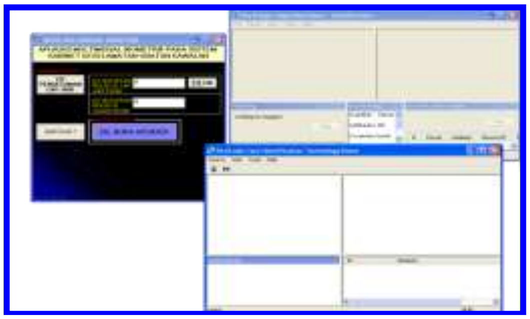


Figure 8: The overall windows of the system.

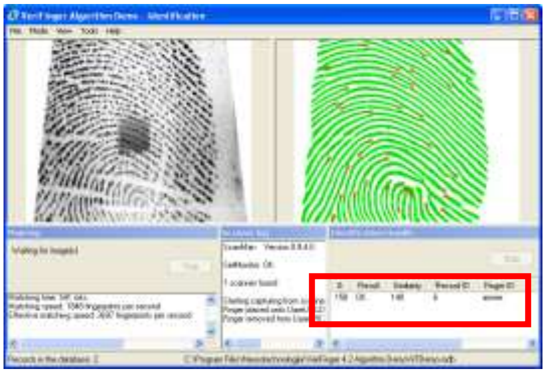


Figure 9: Fingerprint ID appeared for a successful recognition.

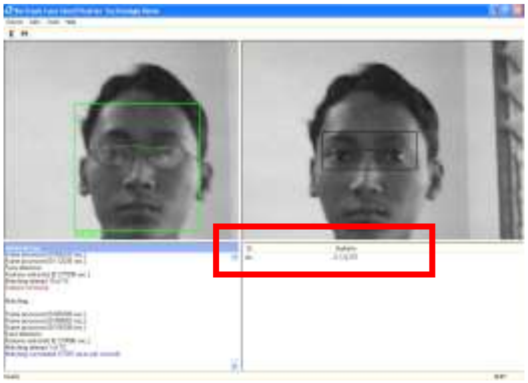
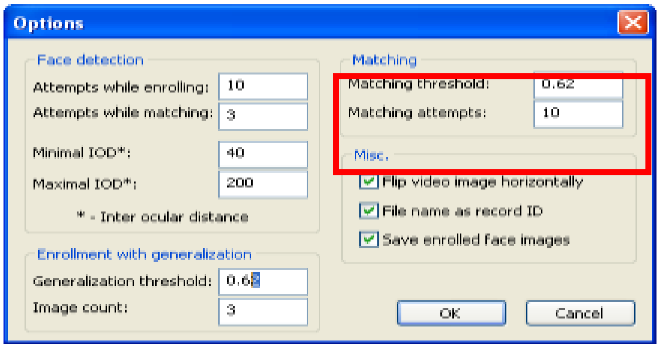


Figure 10: Facial ID appeared for a successful recognition.

4.2 Threshold Value

Figure 11 shows the matching threshold setting of biometric software. The administrator sets the threshold value. Threshold values are not fixed but the values consideration determines the security level possessed. Table 2 shows the study of various level of threshold value. From the study, the moderate threshold level (0.501 – 0.750) provide a suitable value for a security purpose since the range has a suitable low false acceptance rate (FAR, different subject erroneously accepted as of the same) and suitable high false rejection rate, (FRR, same subjects erroneously accepted as different). The FAR is about 0.01%.



Options

Face detection

Attempts while enrolling: 10

Attempts while matching: 3

Minimal IOD*: 40

Maximal IOD*: 200

* - Inter ocular distance

Enrollment with generalization

Generalization threshold: 0.62

Image count: 3

Matching

Matching threshold: 0.62

Matching attempts: 10

Misc.

☑ Flip video image horizontally

☑ File name as record ID

☑ Save enrolled face images

Figure 11: The matching threshold setting.

Threshold level	**Threshold Value**	**Performance**
Low	0 – 0.500	Provide a loose security system. The imposters might be well accepted as the identity of the credential user. Not recommended for security purpose.
Moderate	0.501 – 0.750	It is not too strict or loose system for a security purpose. The value can distinguish between the real authorized user and the imposters. This value is moderate and suitable for commercialize.
High	0.751 – 1.00	The ideal value for security system. In reality, even the credential user might have difficulties to achieve this ideal value. So the credential user as well as imposters will have possibilities been rejected. The value is not recommended.

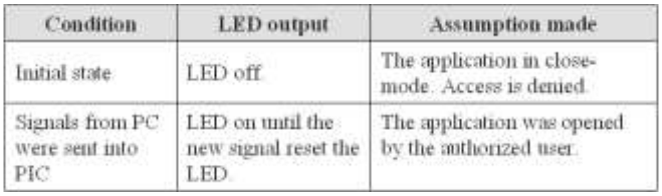
Table 2: The matching threshold value studies

4.3 PIC Programming

The microcontroller used for this project is the 16F84A PIC. It has 35 single word instructions to learn in order to build its program. The PIC contains two output /input ports named A and B with four interrupt sources. In this project, the PIC is used to interface with RS232 through MAX232. RS232 is a standard for serial cable interfaces used for 24 and 9 pin connections. In RS232, a 1 bit is represented by -3 to -25V, while a 0 bit is +3 to +25V. Therefore to connect any RS232 interface to a microcontroller system, a voltage converter or line driver such as MAX232 must be used to convert the TTL logic levels to RS232 voltage level and vice versa. A 9-pin connection is used in this project with full duplex serial communication that enables data transmission/reception to and from the PIC. This way, signals can be transmitted from the PC to the PIC to open the next application and the PC can also receive signals from the PIC for status of application. A LED is attached to port RA1 of the PIC to demonstrate an application is connected to the serial communication circuit.

4.3.1 LED Simulation Output.

LED simulation circuit was assumed as schedule II controlled drug security room in hospital. Table 3 shows the result from the LED simulation circuit and Figure 12 shows the connection between PC and the LED simulation circuit through the serial communication circuit. The initial state of LED is off and when the PIC receives a signal from the PC, it will trigger the interrupt service routine program in the PIC and turned the LED on. The LED can be turned off by pressing the reset button on the circuit.



Condition	LED output	Assumption made
Initial state	LED off	The application in close-mode. Access is denied.
Signals from PC were sent into PIC	LED on until the new signal reset the LED.	The application was opened by the authorized user.

Table 3: LED output and the assumption made.

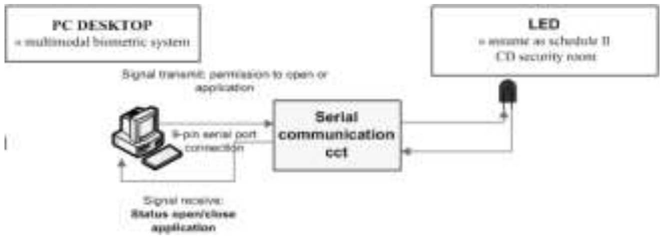

PC DESKTOP
= multimodal biometric system
LED
= assume as schedule II
CD security room
Signal transmit: permission to open or application
9-pin serial port connection
Serial communication cct
Signal receive:
Status open/close application

Figure 12: The connection between PC and the LED simulation circuit.

4.3.2 Power Supply

The voltage regulator IC 7805 is used to fix output voltage. For microcontroller, the maximum voltage is 5V but the power supply that has been used is 9V battery. The voltage regulator has a built-in thermal overload protection which prevents the device from being damaged due to excessive junction temperature. The capacitor is usually added to the voltage regulator circuit to help smooth the noise from the supply line. Figure 13 shows the voltage regulator.

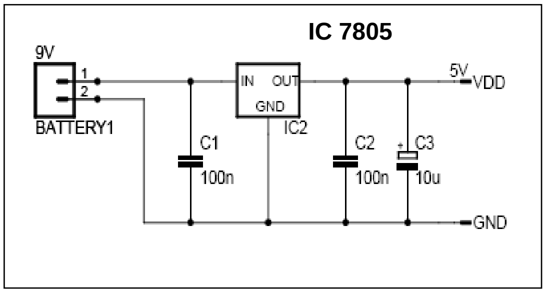


Figure 13: The voltage regulator.

5.0 CONCLUSION

In conclusion, this project is successful in combining two biometric characteristics; fingerprint and facial, in one system to provide higher level of security by enhancing existing password based identification.

A biometric system which is based on a single biometric characteristic may not always be able to achieve the desired performance. A multimodal biometric approach, which combines multiple biometrics in identification process, can be used to overcome the limitations. By combining fingerprint and facial to form a multimodal biometrics security system, it is hope that this method can increase security for physical access to schedule II controlled drug security room.

5.1 Recommendations and Scope for Further Research

There are several improvements that can be implemented into the system of this project. The biometric recognition mode in this project was done using verifinger and verilook software. The softwares can be replaced by designing the source code in visual basic for biometric feature matching. A lot of time, resources and understanding in the concept of image processing using visual basic are needed in order to design the source code.

Testing and experiments can be represented by using the actual room with additional several applications such as magnetic lock, alarm, sensors, the use of CCTV, etc. These additional gadgets can be attached to the PIC for access control by the security system.

REFERENCES

Tabash, M., &Abuqamar, M. (2018). Assessment of The Status Of Private And Non-Governmental Pharmaceuticals Supply Warehouses In Gaza Strip, Palestine. *Assessment*, *11*(2).

Scavia, D. (1995). National Science and Technology Council-Subcommittee on US Coastal Ocean Science. *Setting a New Course for US Coastal Ocean Science*.

Graevenitz, G. A. (2003). Introduction to fingerprint technology. *A&S International*, *53*, 84-86.

Jain, A., Uludag, U., & Ross, A. (2003, June). Biometric template selection: a case study in fingerprints. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 335-342). Springer, Berlin, Heidelberg.

Soobia Saeed, Mahmood Naqvi, & Muhammad Memon. (2020). E-Commerce Web Crawling to Facilitate Consumers for Economical Choices. *International Journal of Advanced Computer Systems and Software Engineering*, *1*(1), 1-13.

Heidelberg. Abiantun, R., Savvides, M., & Khosla, P. K. (2005, October). Automatic eye-level height system for face and iris recognition systems. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)* (pp. 155-159). IEEE.

MohdKamarulEssmanBinMohd Yusof (2006). “Multimodal Biometric Security System.” KolejUniversitiTeknologi Tun Hussein Onn: Tesis.

Shaikh, A. (2020). An Automated Collaborative Online Business Communication System For Desktop Applications. *International Journal of Advanced Computer Systems and Software Engineering*, *1*(1), 14-23.