Paper smart cyber

by Apri Siswanto

Submission date: 23-Oct-2021 09:41AM (UTC+0700)
Submission ID: 1681611792
File name: Two_Factor_Authentication_for_Safe_Deposit_Box.doc (21.48M)
Word count: 3234
Character count: 17713

Two Factor Authentication for Safe Deposit Box Based on Embedded System

Apri Siswanto[1], Akmar Efendi[1], Zalian Hasrin[1], Bustamil Arifin[1]

[1] Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau, Pekanbaru, Indonesia

Abstract. Security is one of the most significant needs for people everywhere. Likewise, people usually use a safe deposit box (SDB) to store valuables for the storage of goods. However, traditional SDB is very easy to open or steal from criminals. For this reason, an effective SDB system is needed to secure valuables. This study proposed a two-factor authentication for SDB based on fingerprint and PIN. The proposed SDB system is secure and more efficient for storage system authentication in embedded system environments. To be able to use the system, the user must register. After being registered in the system, the registered user will perform authentication. The prototype of a safe authentication system provides a basic overview of integrating a fingerprint sensor, Arduino Mega 2560, keypad, and safe deposit box with a simple application. The prototype system that has been designed can be used to solve access control security problems in a safe system. Two alternatives of fingerprint or PIN authentication provide convenience and accuracy for safe authentication systems. It is hoped that this design is an alternative to a cheap SDB and secure to use.

Keywords: Security, Safe Deposit Box, Authentication, Embedded System, Fingerprint.

1 Introduction

Technology security is fundamental in every company agency and individuals—all things, both security in the environment and security for existing data and systems. Security is essential today, because of the increasing number of attacks or crimes, especially in technology. Many security system technologies in the information technology world have been developed for intelligent home security, ATM security, bank security, smart cities, etc. One of the concerns in security is the security of safe deposit boxes (1-3).

A safe deposit box (SDB), also known as a safe deposit locker (SDL), is an individually secured container, usually stored in a safe or more considerable bank vault. Safes are generally located in banks, homes, post offices, or other institutions. Safe deposit box are used to store valuables, such as gemstones, precious metals, currency, securities, luxury items, important documents (e.g., wills, property

certificates, or birth certificates), or computer data, which require protection from theft, fire, floods, disturbances, or other hazards (4-6).

Hotels, resorts, and cruise ships sometimes also offer safes or small safes to their customers for temporary use during their stay (7). These facilities may be located behind the reception desk or securely anchored in private rooms for privacy. The contents of the safe deposit box can be confiscated based on the legal theory of abandoned property. They can also be searched and confiscated by court order by issuing a search warrant (8).

In the development of the safe system, there have also been many developments of the safe security system. Using a safe can secure several valuable objects, including jewelry, money or letters, and valuable documents in a company. The contents of a safe are not easy to retrieve because they require authentication from the owner. But even though you have used safe, criminal acts in the form of theft can still occur. As safe and sophisticated as anything, a safe is easy to steal if the owner is not there (9, 10). Based on this problem, the researcher offers a solution to prevent the theft of the safe and can be controlled automatically. We will develop a dual authentication system for safes using embedded system technology. This dual authentication consists of fingerprint and Personal Identification Number (PIN).

2 Research Method

This study used experimental research methods. In order to obtain optimal results, this experimental research takes the first steps, namely problem identification. The problem is to study literature studies related to authentication systems for safe vaults and embedded systems. Then design the prototype of the tool to be designed. The tools involved are microcontroller, fingerprint sensor, keypad, LCD, and solenoid. After designing the tool prototype, the researcher will conduct experiments by designing hardware and software for a dual authentication system for intelligent safes (11). After that, do the testing and make a report as shown in Figure 1.

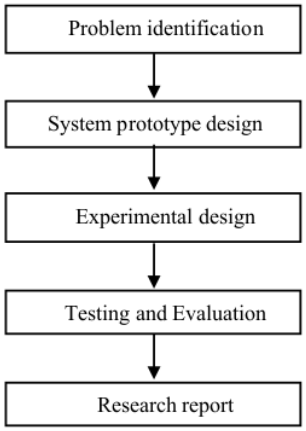

Figure 1. Research method

The prototype design of the two-factor authentication system for this smart safe deposit box consists of tools such as a microcontroller, fingerprint sensor, keypad, LCD, and box for the prototype safe. As in Figure 2.

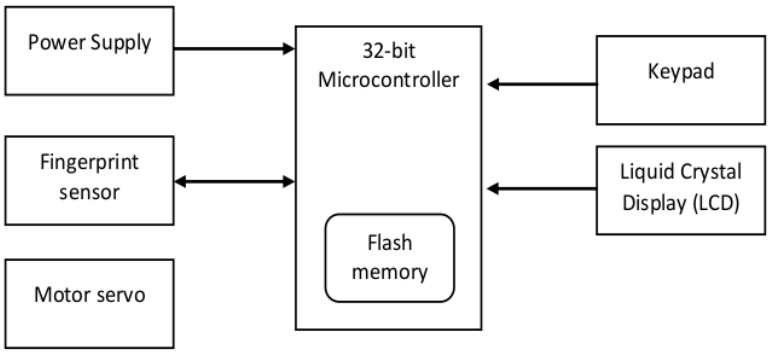

Figure 2. The proposed hardware design of safe deposit box

There are two types of materials employed in this study: hardware and software. The term "hardware material" refers to tangible equipment such as a personal computer (PC), fingerprint optic sensor, microcontroller, door lock, LCD, and power supply that were employed in the study. Software materials are invisible and non-touchable substances. They are virtual objects that are employed in the development of applications. MATLAB, Arduino's integrated development environment (IDE), and C code are examples of software applications. The hardware tools and their specification are presented in Table 1.

Table 1. Hardware tools and specifications

Hardware	Specification	Description
PC	Processor: Core (TM) i7-7500U CPU @2.70GHz (4 CPUs), 2.9 GHz Memory: 8192 MB 64-bit Operating system Harddisk 1 TB Graphics base frequency: 300 MHz	PC used to design software and coding for controlling the system.
Microcontroller		

	Microcontroller ATmega328 USB to Serial Chip Atmel AT16U2 Flash Memory 32 KB (ATmega328) of which 0.5 KB used by boot loader SRAM 2 KB (ATmega328) EEPROM 1 KB (ATmega328) Clock Speed 16 MHz	The microcontroller board serves as the hub of the systems and regulates all input and output activities. It retrieves data from the fingerprint sensors, and then processed, stored in the microcontroller memory.
Solenoid door lock	R1ated Stroke: 10mm Cables Length: 240mm Size: 55×x42×29mm	Solenoid door lock is the hardware that controls the opening and locking the smart safe deposit box
Fingerprint sensor	Image acquisition time: 1S Storage capacity: 1000 Matching Mode: comparison mode (1:1) and search mode (1:N) Character file: 256 bytes Template file: 512 bytes Security level: 5(1,2,3,4,5(highest))	The fingerprint sensor serves as a sensor that receives images of fingerprints. The sensor produces digital data to create a biometric template and stores the data in the database for the first time and an input device for authenticating the fingerprints later
Power supply adapter	Input: 100~240Volt, 50/60Hertz output: 9V, 1A Connector size: 5.5*2.1mm (Approx.) Cable Length: 2m(Approx.)	The power supply function is to provide power electricity to all component in the system
LCD	Interface: I2C I2C Address: 0x27 Supply voltage: 5V PCB Size: 98mm60mm	LCD function is to display the data in safe deposit box system

3 Result and Discussion

This section explains a prototype for fingerprint or PIN authentication technology's automation and security. With its simple installation and inexpensive cost, this system helps people improve security of safe deposit box. Based on the user's fingerprint that has been registered in the microcontroller's database, the system automatically controls (lock and unlock) the safe deposit box.

3.1 Software Design

Software that has been designed could control the opening and closing of doors in an embedded system environment or safe deposit box. The first step in the software design is determining the software requirements of the application to be built, followed by collecting and analysing user requirements. At the same time, it also integrates applications with hardware. Then, the next step is coding and implementation. This stage can also return to the middle stage because the app is built by the program iteration or iteration method, as shown in Figure 3 below.

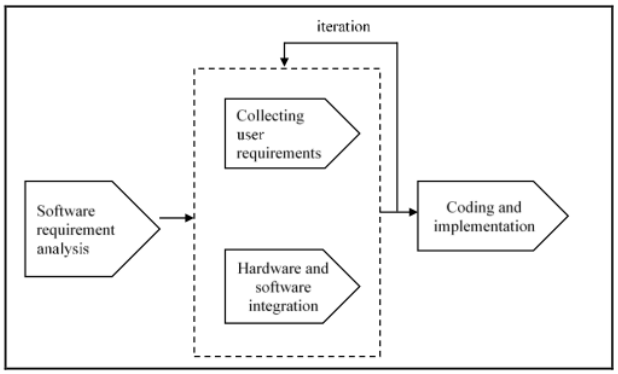

Figure 3. Software design

Software requirements analysis includes conditions, criteria, specifications, or capabilities that must be possessed by the software to fulfil what users require or want (12-14). The aim is to understand comprehensively the existing problem in the software that will be developed, such as the scope of the software product and the users who will use it (15). In this step, the software product which has been designed is the fingerprint door lock security application, with several users. The main requirement for this application is used to register the resident in the system database. After the resident has been registered in the system database, the resident will be allowed to access the legal system environment area through an authentication process. This authentication process also integrates hardware and software. After the hardware and software integration process, the next step is coding and implementation. The code for the prototype is programmed using the Arduino IDE and Proteus tools. Then, product implementation becomes an important phase for user because it provides better control access in the embedded system environment. The software requirement is shown in Table 2.

Table 2. Software specifications

Software	Specification	Function
Operating System Microsoft Windows	Windows Pro 64-bit	Managing computer resources and managing data and programs for doorlock security
Arduino IDE	Arduino 1.8.11	Writing code doorlock security and uploading it to the microcontroller system board
Proteus	Proteus 7.7	Software used to make hardware designs on Arduino Uno which is also equipped with simulations

The software used in this study includes Microsoft Windows operating systems, Arduino IDE, and Proteus. The operating system is to run essential functions on the computer. It regulates the memory usage, data processing, data storage, and other critical computer functions. Then, Arduino IDE writes code and runs Arduino microcontroller. At the same time, Proteus is used to make hardware designs on Arduino Uno which is also equipped with simulation. Then, during the user requirements analysis, four user requirements were identified, which are presented in Table 3.

Table 3. User requirements

User Requirement (UR)	Requirement Specification
UR1	User will be able to enrol fingerprint in the embedded system environment
UR2	User will log in into the embedded system environment by providing fingerprint or PIN
UR3	The system allows access to fingerprints and PINs that have been registered in the system
UR4	The system denied access to fingerprints and PINs not registered in the system

Then, in the hardware and software integration phase, a use case diagram was illustrated. It is a technique to capture business processes from the user's perspective in a embedded system environment. As for the use of the case diagram, the user scans the fingerprint on the sensor device. After it is successful, the user then enters the PIN. After that, it is validated by the admin, so that the user is registered with the system. Admin is the authorized party to determine who has the right to be registered to the embedded system and can access the legal area environment system. For authentication, registered users scan fingerprints or enter PINs. If the data match the database in the microcontroller, access is permitted; if not, access is denied. The details can be seen in Figure 4.

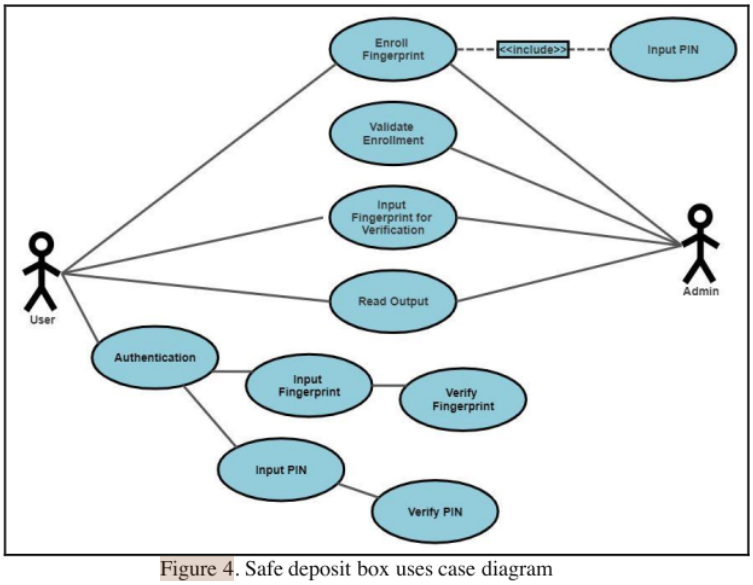

Figure 4. Safe deposit box uses case diagram

This study uses sequence diagrams to explain the sequence of interactions visually by using vertical source diagrams to represent the time the message was sent. In the registration process, the admin first activates the system application so that the user is allowed to register. First, the user enters her/his own PIN, then he/she scans his/her fingerprint. Then, to make sure the fingerprint model is created, the user must put his/her finger again. After the fingerprint data have been successfully recorded into the database, the user will be allowed to access the fingerprint authentication system that has been designed. Figure 5 explains the interaction between the user and objects such as fingerprint sensor, keypad and microcontroller in enrolment and authentication.

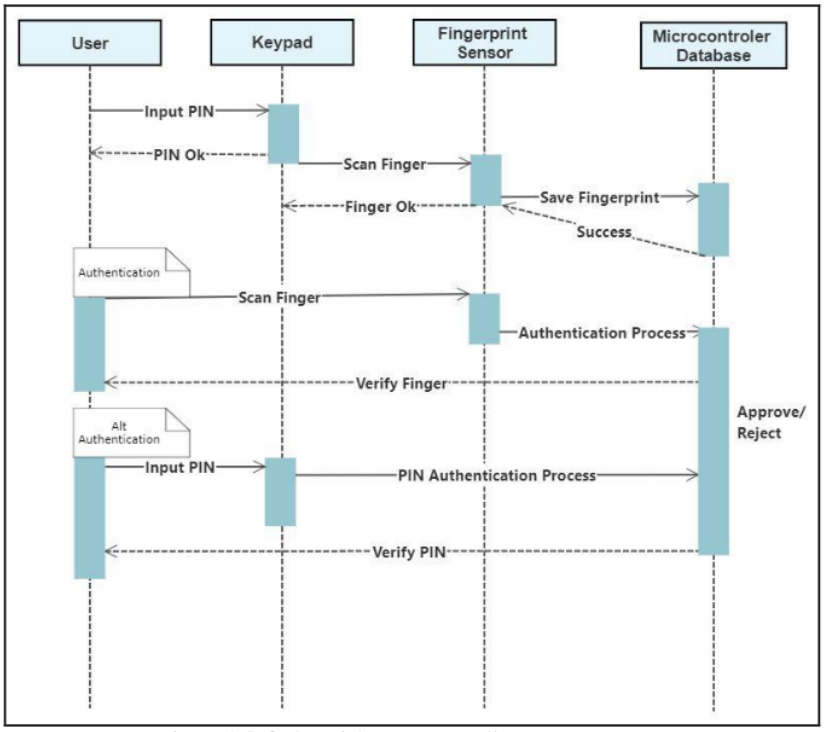

Figure 5. Safe deposit box sequence diagram

Activity diagrams are visual forms of workflows that contain activities and actions, which can also contain choices or repetitions. The activity diagrams are made to explain the interactions between the entities in a system. In addition, the activity diagrams also outline the control flow. Figure 6 explains how the fingerprint authentication system works based on fingerprints or PIN. In these activities, the user can be registered with the fingerprint sensor and the fingerprint template is stored in the microcontroller memory. Then for authentication, registered users are allowed to access the system, while those not registered are denied.

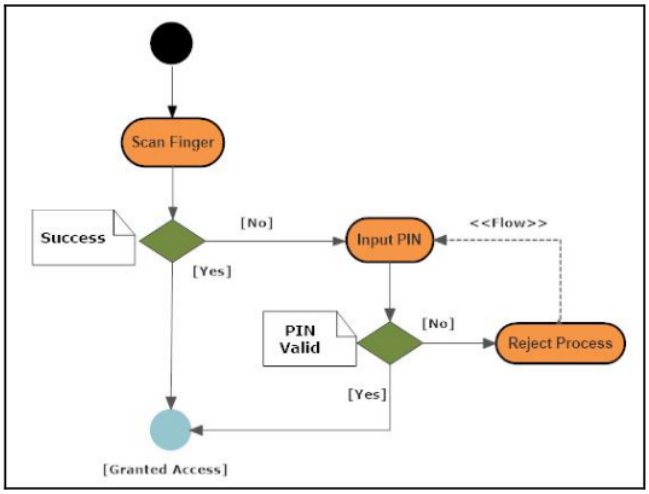

Figure 6. Safe dposit box activity diagram

3.2 Hardware Design and Experimental Study

In this phase, fingerprint sensors are applied to control safe deposit box. When this system is implemented, authorised users are required to register their fingerprint data with a simple application, and the data will be stored in the Arduino microcontroller memory. Users enter PIN and scan their fingerprints using the fingerprint sensor. The scan results are saved in digital format in Arduino memory. After that, fingerprint records are processed by producing a list of unique feature features. The fingerprint pattern feature is stored in a database. When users scan their fingers, the patterns generated from fingerprints will be adjusted to those stored in the database. If the two data match, the Arduino memory sends an approval signal to the microcontroller to open the door lock/electric latch and provide access to the users. The prototype that has been created is shown in Figure 6.

Figure 6. Hardware prototype design

3.2.1 Enrolment Process

In the fingerprint user enrolment process, a user must register his fingerprint into an embedded system, so that it can be recognised in the Arduino Mega 2560 microcontroller database. The steps of the registration process are as follows. First, the user enters her/his chosen PIN, then scans her/his own fingerprint. Then, to ensure the fingerprint model is created, the user must put the finger again. After the fingerprint data have successfully been recorded into the database, the user will be allowed to access safe deposit box that has been designed using the user's fingerprint or PIN that has been enrolled in the database. Figure 7 demonstrates the flow chart of the fingerprint enrolment process.

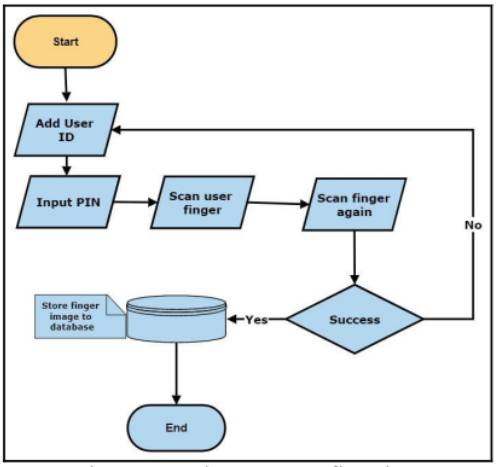

Figure 7. Enrolment process flow chart

There are three steps in managing the enrolment process to the prototype in a safe deposit box embedded system. The first is the display process in choosing whether to add, delete, open or exit in the embedded smart-home system. Press “Add” button to add a new user, then input the PIN of the new user. Then, place the finger on the sensor two times and the fingerprint data will be registered in the embedded system. The prototype was designed as shown in Figure 8.

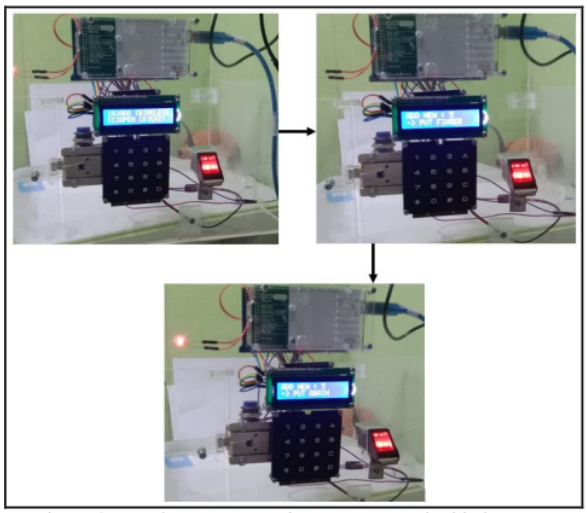

Figure 8. Enrolment process in prototype embedded system

3.2.2 Authentication Process

After being successfully recorded into the database, the user fingerprint template which has been registered in the system will be allowed to access the prototype of safe deposit box embedded system. The user scans his/her finger in a fingerprint sensor. Then, the system will verify whether the data model matches in the database. If it is appropriate, the door/solenoid will open, whereas if it does not match, it will be rejected. In the case if the sensor fails to read the fingerprint data due to dirty or injured hardware or fingers, the user can use the PIN which has been enrolled in the database to open the key. Then, the system built also provides handling to delete the user desired by the homeowner. The flow chart of the developed prototype system is displayed in Figure 9.

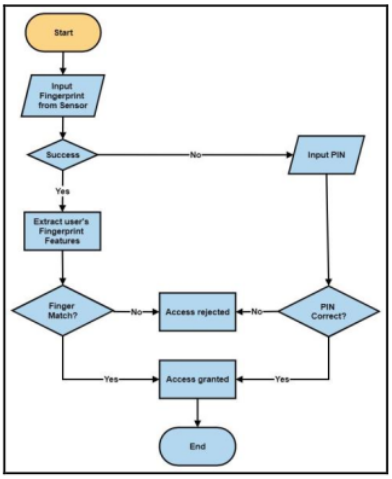

Figure 9. Authentication process flow chart

Authentication mechanisms are now predicated on smart cards, which will invariably result in a slew of security issues if smart cards are lost. Applying authentication with the proposed fingerprint system or PIN protocol could resolve security problems caused by stolen/loss of smart cards. The authentication process in the prototype safe deposit box embedded system designed is shown in Figure 10. If the fingerprint pattern reading is invalid, and the user is not registered in the system database, then the LCD will display the words "access denied" and the solenoid still locks. Figure 10 shows denied access.

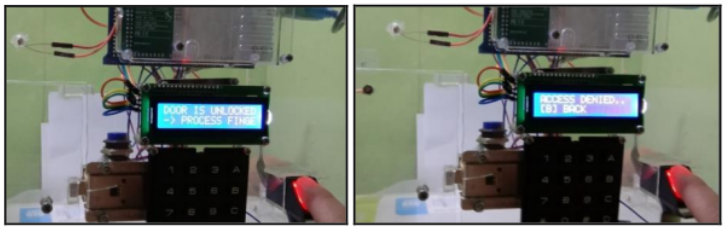

Figure 10. Authentication process and invalid authentication process

Based on the evaluation conducted with several user fingerprints, this prototype can work well in enrolment and authentication process in the database. Table 4 shows the testing of user fingerprint prototypes in SDB embedded system. In the enrolment process stage, the user determines a PIN and performs fingerprint scanning twice. Authentication on the table uses fingerprints only without a PIN.

Table 4. User enrolment and authentication of fingerprint processing time

User fingerprint	Enrolment Processing time (sec)	Authentication Processing time (sec)
Thumb	3.5	2
Index finger	3.5	2
Middle finger	3.5	2
Ring finger	3.5	2
Pinkie	3.5	2

The enrolment and authentication time of SDB is 3.5 seconds and 2 seconds. In contrast, the Murillo-Escobar et al.'s (2015) scheme needs 2.2 and 3.1 seconds for enrolment and authentication, respectively. However, in cases the fingerprint sensors fail or the user's finger is injured (dirty) and get invalid to access or open doors in the home environment, the user can use a PIN as an alternative to access the embedded system as shown in Figure 11.

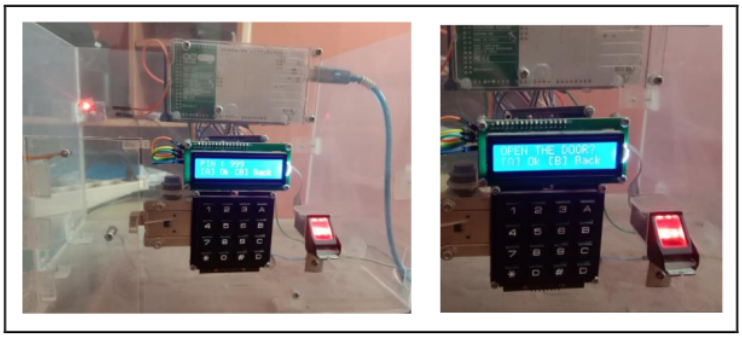

Figure 11. User authentication process using PIN

4 Conclusion

This study succeeded in designing an authentication system for fingerprint and PIN-based safes. The proposed fingerprint authentication system is secure and more efficient for vault system authentication in embedded system environments. To be able to use the system, the user must register. After being registered in the system, the registered user will perform authentication. The prototype of a safe authentication system provides a basic overview of integrating a fingerprint sensor, Arduino Mega 2560, keypad, and safe deposit box with a simple application. The prototype system that has been designed can be used to solve access control security problems in a safe system. Two alternatives of fingerprint or PIN authentication provide convenience and accuracy for safe authentication systems.

References

1. Siswanto A, Katuk N, Ku-Mahamud KR. Biometric fingerprint architecture for home security system. 2016.
2. Jurcut AD, Ranaweera P, Xu L. Introduction to IoT security. IoT security: Advances in authentication. 2020:27-64.
3. Raj P, Raman AC. The Internet of Things: Enabling technologies, platforms, and use cases: CRC Press; 2017.
4. Puspita H. DETEKTOR PROXIMITY SEBAGAI ALAT PENGAMAN BRANKAS. Jurnal Industri Elektro dan Penerbangan. 2020;1(3).
5. Romadhoni MAW, Majdi N, Asri P. Smart Safe Deposit Box Based on Internet of Things. Indonesian Journal of Engineering Research. 2021;2(1):18-22.
6. Warohman SAS. Designing and Testing Safe-deposit Box Safety System Based on Android and Pi Raspberry: University of Technology Yogyakarta; 2020.
7. Medlik S. Dictionary of travel, tourism and hospitality: Routledge; 2012.
8. Sajić M, Bundalo D, Bundalo Z, Stojanović R, Sajić L, editors. Design of digital modular bank safety deposit box using modern information and communication technologies. 2018 7th Mediterranean Conference on Embedded Computing (MECO); 2018: IEEE.
9. Kim H-C. A Study Medium-based safe File Management Security System on the cloud Environment. Journal of Convergence for Information Technology. 2019;9(1):142-50.
10. Kwon D, Yi H, Cho Y, Paek Y. Safe and efficient implementation of a security system on ARM using intra-level privilege separation. ACM Transactions on Privacy and Security (TOPS). 2019;22(2):1-30.
11. Blessing LT, Chakrabarti A. DRM, a design research methodology: Springer Science & Business Media; 2009.

12. Tams S. Good management and software design can help older workers thrive with IT-based tasks. LSE Business Review. 2021.
13. Foster EC. Software Engineering: A Methodical Approach: Auerbach Publications; 2021.
14. Budgen D. Software design: Pearson Education; 2003.
15. Aurum A, Wohlin C. Requirements Engineering: Setting the Context. In: Aurum A, Wohlin C, editors. Engineering and Managing Software Requirements. Berlin, Heidelberg: Springer Berlin Heidelberg; 2005. p. 1-15.

Paper smart cyber

ORIGINALITY REPORT

12%	11%	2%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repo.uum.edu.my Internet Source	4%
2	en.wikipedia.org Internet Source	4%
3	www.dfrobot.com Internet Source	1%
4	www.slideshare.net Internet Source	1%
5	www.scitepress.org Internet Source	<1%
6	Jinxiang Zhang, Qi Wang, Ying Pan, Xu Liu. "Research on Archives Information Management System Based on Computer Big Data", 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), 2021 Publication	<1%
7	real-j.mtak.hu Internet Source	<1%

8	www.freepatentsonline.com Internet Source	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		