Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 13. No. 2, 2025 Series

Article Citation Format
Saliu, L., Sodiq, K., Jumah, A.G., Otapo, A. Otunubi, V., Igwe, N. & Tokunbo-Cole M. (2025): Design and Implementation of a Fingerprint-Based Access-Controlled Aluminum Bookshelf with Integrated Surveillance. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 13, No. 2. Pp 59-72. www.isteams.net/digitaljournal dx.doi.org/10.22624/AIMS/DIGITAL/V13N2P5

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 17th March, 2025
Review Type: Blind Peer
Final Acceptance:12th May, 2025

Design and Implementation of a Fingerprint-Based Access-Controlled Aluminum Bookshelf with Integrated Surveillance

[1]Saliu Lateef, [2]Sodiq Kazeem, [3]Jumah Abdul Ganiyu, [4]Otapo Akeem [5]Otunubi Victor [6]Igwe Ndubuisi & [7]Tokunbo-Cole Mary
[1,2,4,5,6,7]Department of Computer Engineering, Yaba College of Technology Lagos, Nigeria
[3]Department of Mechatronics Engineering, Yaba College of Technology Lagos, Nigeria
E-mails; lateef.saliu@yabatech.edu.ng, jumahga@gmail.com, akeem.otapo@yabatech.edu.ng, victor.otunubi@yabatech.edu.ng, ndubuisi.igwe@yabatech.edu.ng
Corresponding Author: kazeem23@yahoo.com

ABSTRACT

Accurate identity verification is increasingly essential, yet conventional security measures such as passwords and smart cards remain vulnerable to breaches. Fingerprint-based biometrics provide a more secure solution due to their uniqueness and stability. This research develops an automated security system combining fingerprint access control with remote IP camera monitoring to prevent book theft in academic settings. Utilizing a ZKTecoX6 fingerprint reader, an electromagnetic lock, and a 360° smart camera, the system ensures restricted access while enabling real-time surveillance via the V380 PRO app. Built with aluminum for durability, the system was tested under various scenarios, successfully granting access to authorized users while triggering alarms for unauthorized attempts. The findings support the effectiveness of biometric security in protecting institutional resources, with recommendations for further improvements, such as automated doors and fireproof materials. The study advocates for the adoption of electronic bookshelves in higher education institutions to enhance security.

Keywords: Biometric Security, Fingerprint Access Control , Remote Survellance, Aluminium Bookshelf, Smart IP Camera.

1. INTRODUCTION

Accurate personal identification is becoming increasingly vital nowadays. The usual methods (smart cards, passwords (Adegun et al.(2014)) have demonstrated their limitations (falsification, loss). Biometrics (the study of a person's biological features) may provide a satisfactory solution to these issues. Fingerprint recognition is now the most frequently utilized method of personal identification. Fingerprints are a one-of-a-kind, permanent global pattern made up of geographically parallel ridges connected by single points (minutiae) (Chandana et al., 2015). Ink and paper were used for a long time to create an image from a finger. Nonetheless, developments in technology have allowed the acquisition stage to be automated utilizing solid-state sensors.

These sensors gather images using a number of ways (pressure, electrical field, temperature), and they require either a static (matrix sensor) or mobile finger position (sweeping mode sensor). Various control methods have been developed to prevent unauthorized people from gaining access DICE (n.d) .The primary purpose of installing locks in our structures is to ensure the safety of people and property. As a result, having a stress-free and straightforward method of accomplishing this goal is critical. Doors and shelves that open automatically have become a regular feature on various structures. They are growing in popularity every day in creating practical electrical gadgets aimed at providing appropriate protection.

Because of the massive growth in crime, home security has become a significant source of concern, and everyone wants to take adequate precautions to avoid entry or unwelcome users. Furthermore, there was a need to automate the house so that users might benefit from advances in real-time technology and computer control systems (Elkholy et al., 2022). It's also worth noting that a keypad and biometric system may be used in the home or workplace to control equipment like doors, shelves, light bulbs, televisions, air conditioners, and robotic arms.

Finally, by inventing and implementing programmable passwords and biometrics locks, the issues of producing electronic gadgets without a corresponding locking system have been addressed. Unquestionably, this will serve as a measure to extend the life of such electronic devices as well as to ensure adequate safety and required protection of data, files, electronic devices, and a variety of facilities such as computer systems, television, and, most importantly, to provide a means of restricting and disallowing unauthorized users from gaining access to an automobile car through the ignition system(LENEL.S2,2025).

Despite all types of security devices and locks, the rising prevalence of crime, attacks by thieves, intruders, and vandals still require the attention of researchers to provide a lasting answer to the well-being of lives and properties of persons. To prevent unauthorized individuals from gaining access to one's property through the use of keys, a low-cost and effective security system is being developed for buildings, automobiles, safes, shelves, doors, and gates.

The need to provide adequate security and safety of educational “items” particularly books cannot be overemphasized especially in Higher Education Institutions. In recent times, there have been cases of stolen books in the Main Library of Yaba College of Technology without anybody to hold accountable for the missing books except for the staff in-charge. Some of the books are costly and scarce to get and such need to be properly kept and secured. There is therefore a need to implement a system where activities around bookshelf can be easily monitored and restrictions from unauthorized persons are put in place using a fingerprint access control on an aluminum bookshelf and also monitoring it remotely using a smart IP camera.

2. RELATED WORKS

According to Baidya et al. (2017) who worked on "Design and Implementation of a Fingerprint Based Lock System for Shared Access” discussed a smartphone-based fingerprint security system." The authors explained that the system can be set up to connect to those phones and open doors using voice commands. Finally, the authors stated that fingerprint ID is now used in the majority of new phones. That fingerprint ID-based phones will soon be ubiquitous, with almost everyone possessing one, and that this security feature will be quite useful. It is recommended that smartphones with the most modern features use a fingerprint ID system to gain access to the device.

According to Amuda and Tennyson (2017) who worked on “Design and Implementation of a Fingerprint Lock System” .The authors noted that fingerprint locking system based on a microcontroller operates by using fingerprint recognition to verify an image before unlocking the electronic lock. This study focuses on the development of a fingerprint verification system utilizing Arduino version 1.6.3. The verification process involves comparing the stored fingerprint data of authorized users with the newly captured fingerprint. Before comparison, the incoming fingerprint image undergoes extraction and filtering procedures to retrieve relevant information for identification. The fingerprint module was programmed to recognize and determine whether an incoming fingerprint image is authentic or fraudulent. Fingerprint recognition has wider applications in personal authentication, such as gaining access to a computer, network, ATM, vehicle, or residential property.

Ajinkya (2013) worked on "Fingerprint-based locking system," and stated that fingerprints are "patterns of ridges and valleys on the surface of the finger," which are generated by a combination of genetic and environmental influences, just like everything else in the human body. The genetic coding in DNA provides overall instructions on how a developing fetus' skin should develop, but the precise details. With the use of an interface, fingerprints can be utilized to create secure and impenetrable door locks and numerous lock systems. Interfacing is the process of connecting a Microcontroller to an interface. Fingerprint interfaces can be used with any microcontroller and are ubiquitous. It is made up of two parts: hardware (the interface) and software (i.e., the source code to communicate, also called the Driver).

Manisha et al.(2020) who worked on “Design and Implementation of a Fingerprint Based Lock System for Shared Access” , used an R305 fingerprint scanner connected to an Arduino microcontroller (ATMEGA328P) to manage the door's locking and unlocking functions. Throughout the door’s opening and closing operations, a 16x2 Liquid Crystal Display (LCD) presents various instructions to guide the user, such as "Place your finger on the sensor," "Door opened," "Door closed," "Message sent," and "Please enter the password." If an unauthorized individual attempts to access the door using an unregistered fingerprint, access is automatically denied. The proposed fingerprint-based door security system is suitable for use in homes, offices, banks, hospitals, as well as in both governmental and private sector facilities.

Omijeh and Ajabuego (2013) noted that access to doors is typically managed using indoor locking systems [2]. However, with continuous advancements in all areas of modern life and the increasing digitization of our environment, protecting sensitive information has become increasingly difficult. Traditional security measures, such as passwords and physical keys, were once regarded as adequate for securing data and controlling access, but they are no longer sufficient in today’s digital age.

3. METHODOLOGY

The figure 1 shows the framework of the system.

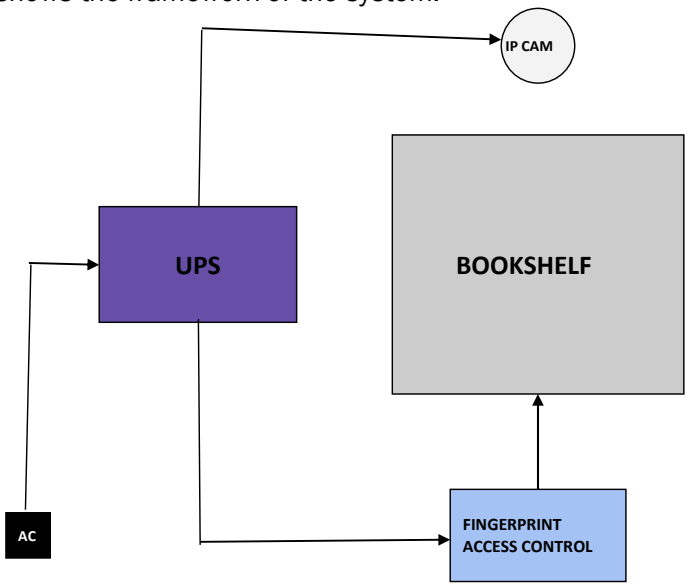

Figure 1: Framework of Aluminium Bookshelf System

In this framework, the UPS is plugged to the mains while the smart camera is plugged to the UPS and also the fingerprint for backup power supply. The fingerprint access control is mounted on the door of the aluminum bookshelf. The fingerprint access control device is ZKTecoX6 Fingerprint RFID Card Access and was installed as a standalone device or as part of a larger access control system. It grants access through valid PINs, fingerprints, or RFID cards.. The Single Door 12V Electric Magnetic Lock 280KG (350LB) was used to lock the Bookshelf. The uninterrupted power supply is the DC13.5V 5A used to provide uninterruptible power supply to the system. The UPS Battery used for the Access control was the 12v 7ah Replacement battery. The IP camera i.e Panoramic IP Camera 360° - 1080P RES Motion Detection-White was used to provide a panoramic view that spans 360 degrees.Also , a smartphone was needed for the remote monitoring of the bookshelf through the IP camera.

In addition to this, the two main softwares used are the operating system(Android/IOS) and the V380 PRO, which is used to remotely monitor the bookshelf through the IP camera.Android and IOS-enabled smartphones were used to test the IP camera remotely and they both worked perfectly.V380 PRO was used for video monitoring utility app for real-time alarms and notifications on whatever your motion-tracking security camera has been detected. Aluminum bookshelf for this research work was constructed with the following glass, partition board, hook, picket, divider, shelf-stand, screws, plastic angle, key lock, blazing rubber, 40 x 40mm aluminum curve, handle.In addition, tools such as drilling machine, cutting machine, milling machine, iron saw, protective glass, hand gloves, protective boot, screwdrivers and 4mm, 3.5mm 6mm drill were used for the construction of Aluminum bookshelf.

The procedures involved in the construction of the shelf are as follows:

a. Cut up four pieces of the 140mm x 140mm of the aluminum curve for the length of the shelf, cut also four pieces of 1750mm and four pieces of 1100mm aluminum curve, and finally cut four 5 length beads of the aluminum curve which makes up the frame of the shelf.
b. Attach each piece to plastic handles at the corners of the bookshelf to form the structures of the bookshelf.
c. The mullion (1750mm) is used to divide the shelf vertically into two equal parts.
d. The shelf has one compartment and it's divided into four steps which the partition board is made to rest on each step. The blazing rubber is used to hold the board and prevent shaking. One of the compartment's two doors includes a magnetic lock, and it will be utilized to automate the bookshelf.

3.1 Implementation

3.1.1 Installation and Configuration of Fingerprint Access Control on the Aluminum Bookshelf

The following are the installation (Figure 2) and configuration of Fingerprint Access Control
Step 1**:** Unscrew the bolt located at the base of the fingerprint access control unit.
Step 2: Remove the back panel.
Step 3: Attach the back panel to the bookshelf

Figure 2: Installation of Fingerprint Access Control

Step 4: Connect the Fingerprint wire (figure 3) to the UPS using a CAT6 network cable
Step 5: Fix the device to the back.

3.1.2 Installation of the Magnetic Lock

Step 1: Remove the screw from the top of the device
Step 2: Connect the Magnetic lock to the UPS power supply using the networking cable

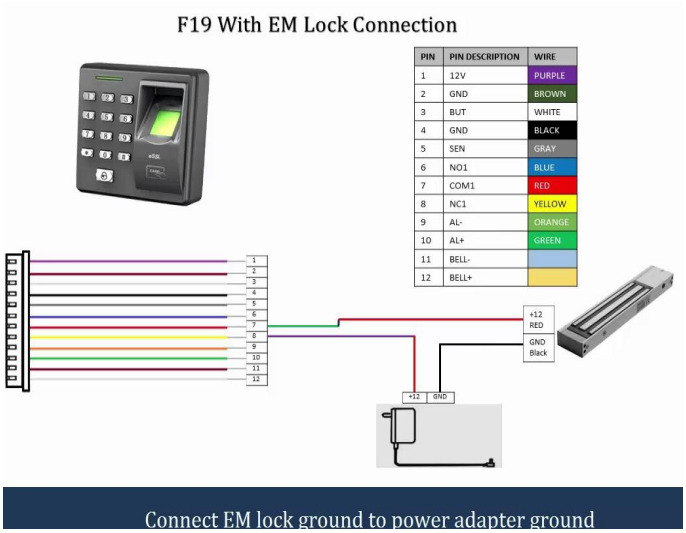

Figure 3: Wiring diagram of the Fingerprint Access Control

3.1.3 Configuration of the fingerprint access control

1. Buttons represent: [#] means yes, [*] means Escape
2. Lights represent: Green means success, Red means Failure
3. Number: Password=4 digits, work code<=5 digits
4. Tones: Long buzz means success, short buzz twice means failure, short buzz 4 times means the wrong action

And [#] must be pressed to confirm, and [*] exit to initial condition

3.1.4 Installation and Configuration of the Smart Camera
iPhone IOS Smartphone Installation
1. search , open Apple App Store, download, and install V380 pro shown in figure 4.

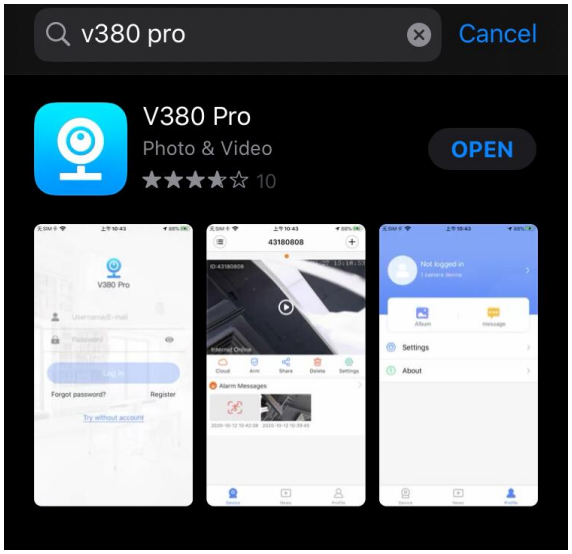

Figure 4: V380 PRO in App store

2. Plug the power cable into the camera and position the camera close to your Wi-Fi router.
   - The camera will announce: *"System is starting"*
   - Followed by: *"System startup completed"*

3.Press and hold the reset button located at the back of the camera until you hear the following prompts:
   - *"Restore factory default setting"*
   - *"Waiting for WiFi smart camera link configuration"* (see Figure 5)

4. launch the app V380

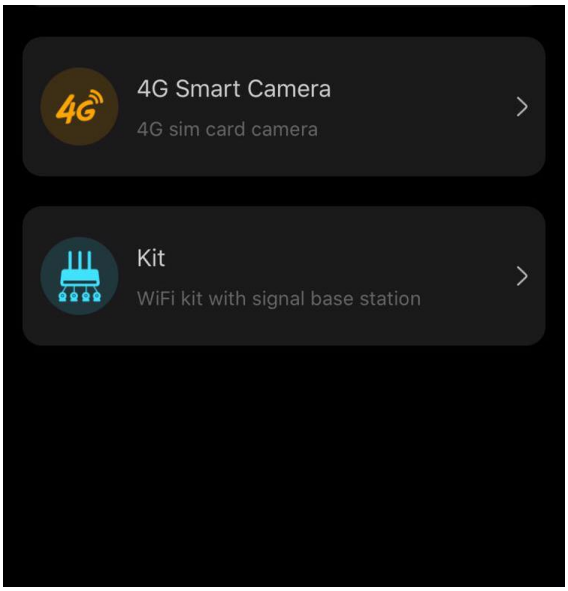

Figure 5: Selection of WiFi smart camera

Click on "Add Device ID"

5. Ensure phone is connected to the camera's access point. On the next screen, you can either tap “LAN Search” or manually enter the Device ID (found on the bottom of the camera, see Figure 6), then click “Add to list” to include the camera in your device list.

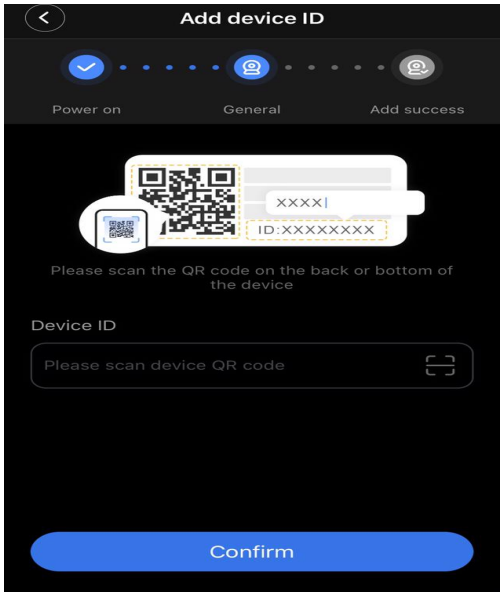

Figure 6: Adding device ID

6. When the phone successfully connects to the camera, the smart camera (figure 7) will be shown on the Device List.

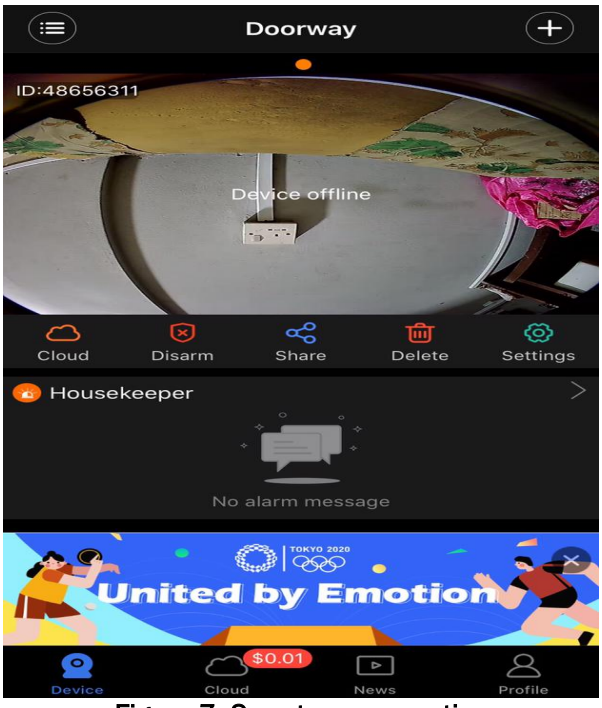

Figure 7: Smart camera active

Now the camera is set up, for direct connection, the camera can only be accessed when your phone is within range of the camera's access point signal. To set up the camera on a Wi-Fi network, place it close to your Wi-Fi router and proceed with the following steps.

7. Successfully Installed
3.2.6 Android Smartphone Installation
WiFi Smart Link Setup (Using a WiFi Network)
1. Go to the Google Play Store, search for V380, then download and install the app (see Figure 8)

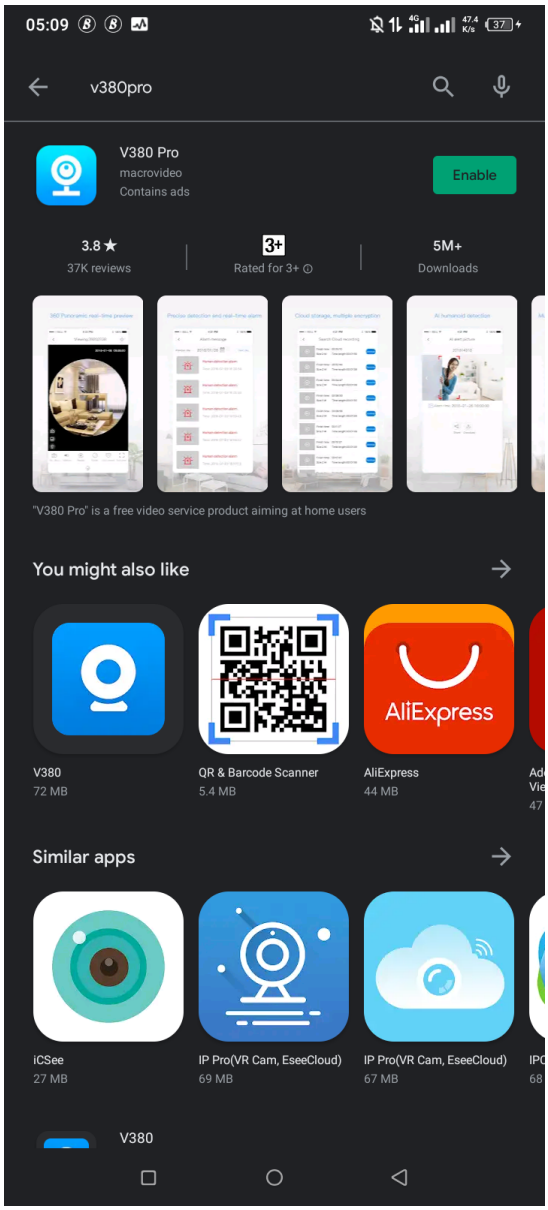

Figure 8: V380 PRO in Google play store

2.Plug the power adapter into the camera and position the camera close to your Wi-Fi router.

The camera will announce: “System is starting”

Then: “System startup completed”

3.Press and hold the reset button on the back of the camera until you hear the following prompts:

“Restore factory default setting”

“Waiting for WiFi smart link configuration”

4.Open the app V380 and Register
Click on “Add Device ID” (figure 9)

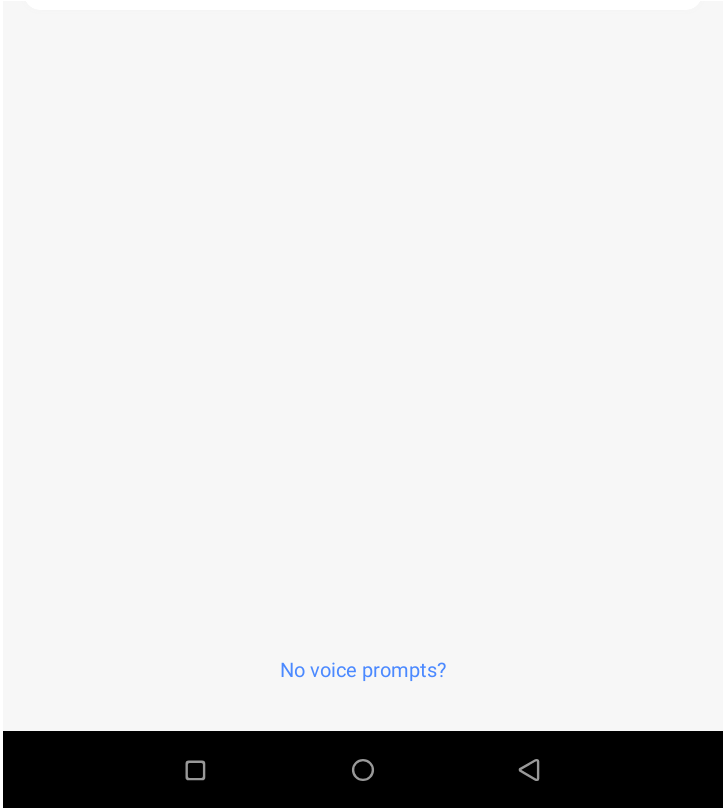

Figure 9: Click on Device ID

5. The phone has to be connected to the smart camera wifi before entering your Device ID(figure 10).

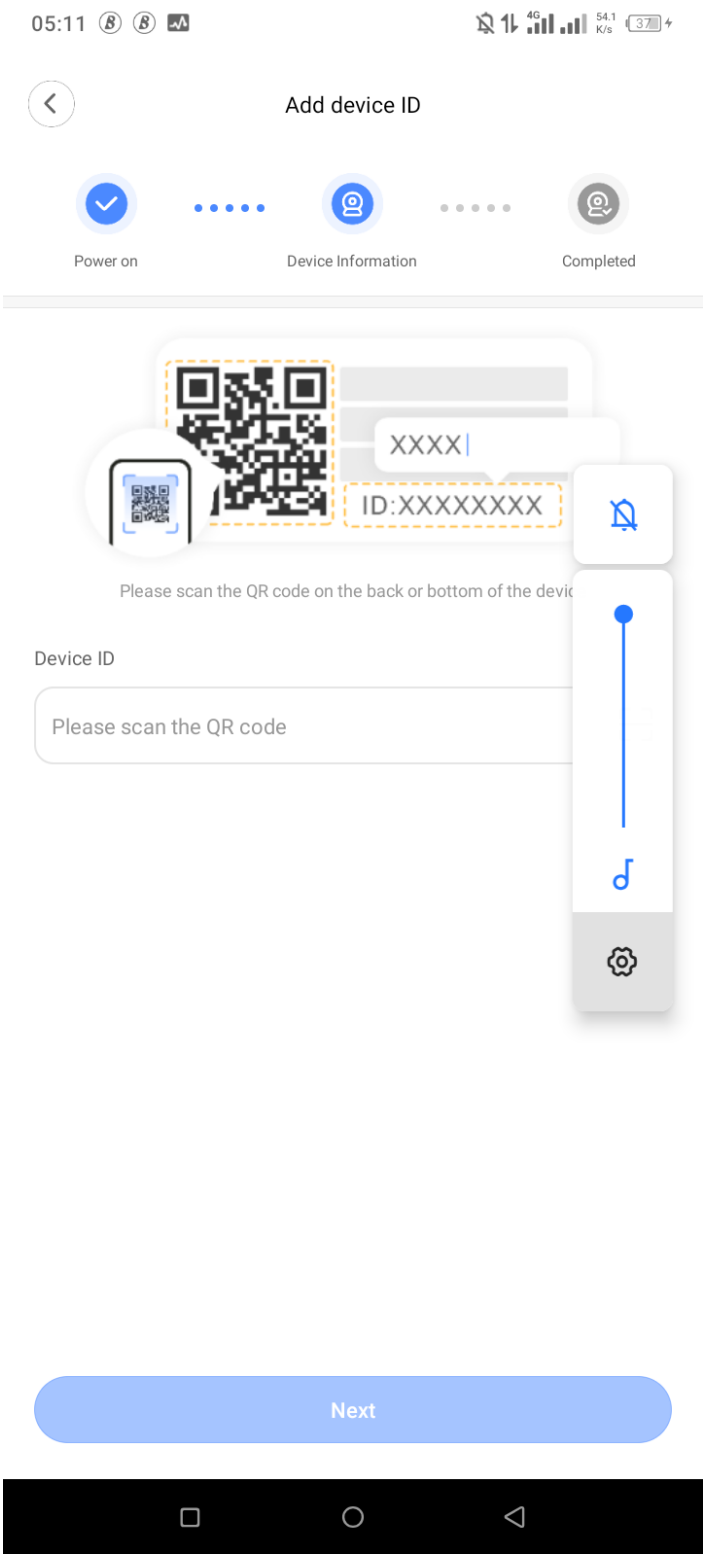

Figure 10: input device ID

6. Successfully installed

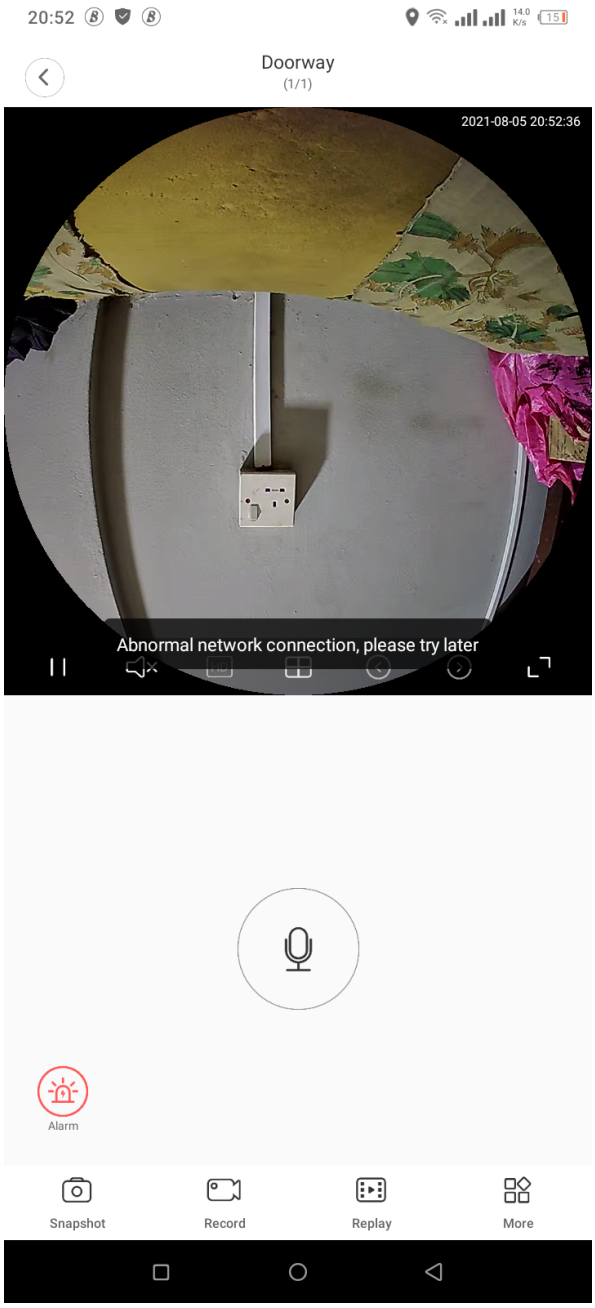

Figure 11: Smart camera working perfectly

3.2 Principle of Operation

When the fingerprint access control is active and a registered user input his or her finger on the fingerprint sensor, the magnetic Lock will neutralize making it possible to access the bookshelf and the magnetic Lock becomes active when the door of the bookshelf is shut.

4. RESULT AND DISCUSSION

Testing as shown in table 1 was conducted at different times of the day taking records of the smart camera and fingerprint access control functionality. Different scenarios were analyzed such as recording unauthorized access to the bookshelf and the corresponding warning signal obtained from the fingerprint access control and smart camera.

Table 1: Test Outputs

Date and Time	Test carried out	Alarm type	Remark
3-08-2024, 9:25	An unauthorized user accessing the bookshelf	Long beep by the fingerprint access control	Satisfactory
4-08-2024, 13:18	Authorized user	Granted access	Satisfactory
5-08-2024, 10:05	An unauthorized user accessing the bookshelf	The smart camera triggered an alarm	Fair
5-08-2024, 15:24	Authorized user	Granted access	Satisfactory

From the test carried out, it was observed that the fingerprint access control did not grant access to an unregistered user and alarm was also triggered through the smart camera using the V380 pro app.The first row in the table shows that a person whose fingerprint was not registered on the fingerprint based access control was denied access to the bookshelf. The second row shows a person whose fingerprint was registered on the fingerprint based access control and was granted access. The third row shows remote monitoring while an unauthorized user was trying to access the shelf and the smart camera alarm was triggered . And the fourth row shows that authorized user accessing the bookshelf was monitored.

5. CONCLUSION

In this research, a system was developed to prevent unauthorized access to books by integrating fingerprint-based access control with a surveillance mechanism. Aluminum was chosen for the construction of the bookshelf due to its durability and longevity. Future enhancements to the system may include the incorporation of an automated sliding door mechanism using a motor, thereby improving usability. Additionally, combining physical and information security measures is suggested to further strengthen the security of the bookshelf. To enhance resistance against external threats, materials such as fire-resistant steel and bulletproof glass may be considered. It is recommended that, in order to ensure organized book management and improved security, every office in tertiary institutions should be equipped with an electronic bookshelf.

REFERENCES

Adegun A.A., Adigun A. and Asani E.O. (2014). A Review Of Trends Of Authentication Mechanisms for Access Control . Computing, Information Systems, Development Informatics & Allied Research Journal. Vol. 5 No. 2. June 2014 – www.cisdijournal.net .

Ajinkya Kawale (2013). Fingerprint based locking system. International Journal of Scientific & Engineering Research, Volume 4, No 5, pp. 899 -900, May-2013 .

Amuda F.A. and Tennyson D.I.(2017). Design and Implementation of a Fingerprint Lock System. IOSR Journal of Engineering. ISSN (e): 2250-3021, ISSN (p): 2278-8719

Vol. 07, Issue 04 (April. 2017).|

Baidya, J., Saha, T., Moyashir, R. and Palit, R. (2017). Design and implementation of a fingerprint based lock system for shared access. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448 .

Chandana , Yadav,S. and Mathuria,M.(2015). Fingerprint Recognition based on Minutiae Information. International Journal of Computer Applications (0975 – 8887). Volume 120 – No.10, June 2015.

DICE (n.d) Seven Ways to Prevent Unauthorized Access to your Company Data . Retrieved from https://dicecommunications.com/seven-ways-to-prevent-unauthorized-access-to-your-company-data Elkholy, M. H., Senjyu, T., Lotfy, M. E., Elgarhy, A., Ali, N. S., & Gaafar, T. S. (2022). Design and Implementation of a Real-Time Smart Home Management System Considering Energy Saving. *Sustainability*, *14*(21), 13840. https://doi.org/10.3390/su142113840 .

LENEL.S2 (2025).How to Prevent Unauthorized Physical Access in the Workplace Retrieved from https://www.lenels2.com/en/news/insights/How_to_Prevent_Unauthorized_Access.html .

Manisha, K., Divya, D., Premalatha, B., Nandhini, A. and Krishnamurthy, A. (2020). Design and Implementation of a Fingerprint Based Lock System for Shared Access. International Journal for Advanced Research in Science and Technology. Volume 10, Issue 12, Dec 2020. ISSN 2457 – 0362.

Omijeh B., Ajabuego G. (2013). Design Analysis of a Security Lock System Using Pass-Code and Smart-Card. IOSR J Elect Comm Eng 4: 64-72.