IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 11, No. 2, 2022
www.ijdieret.in

(Research Article)

Mobile Automation of Key Collection System Using Device Biometric

J. A. Oladunjoye[1*], T. Moses[2]

[1*]*Department of Computer Science, Federal University, Wukari, Taraba State, NIGERIA*
[2]*Department of Computer Science, Federal University of Lafia, Nasarawa State, NIGERIA*

Abstract

It is impossible to overstate how much the advancement of technology has impacted our culture and day-to-day activities. Technology is essential for completing tasks quickly, effectively, and efficiently. Its expansion has resulted in widespread dissemination across several disciplines. The development of biometric technology has improved record authenticity, hence enhancing the integrity and uniqueness of individual records. Every organization places a high value on key management. An efficient key management system offers key records on demand, making it simple to maintain track of the organization keys and the people who signed them. The Dalhatu Araf Specialist Hospital in Lafia uses a manual approach for key collection with staff members signing up on handwritten forms. The goal of this project is to automate the manual process and include biometric thumb printing as a means to accurately monitor the whereabouts of signed keys. The study uses the structured system analysis and design methodology as a tool to structurally guide the goal of this study in order to construct the targeted system efficiently. The system being targeted is a mobile application that utilized Java with SQLite database technology.

Keywords: Key Collection Management, Device Biometric, Mobile Key Collection, Signed Key Records.

1. Introduction

The world has undergone a revolution as a result of the spread of internet technology [1]. Its expansion has had a significant influence on several academic departments and disciplines; Artificial Intelligence, machine learning, robotics, bioinformatics, biomedicals, etc. are all included in this discipline [2-4]. Utilizing devices like a biometric thumbprint are crucial for enhancing the security and uniqueness of organizational records. The benefit of using biometric security systems over more traditional authentication techniques, including personal identification cards, magnetic cards, and individual names, is obvious: they are inextricably tied to a person and consequently difficult to be compromised by loss, fraud, or theft thus, enhancing a system's security and dependability.

Physical asset security for organizations is a developing trend with a persistent demand for high-performance. Unified solutions that are affordable and can assist to maintain a secure working environment are necessary in organizations. With a broad variety of options and capabilities, modern key management systems in particular satisfy those demands, making them even more helpful and safe for today's security requirements.

Any firm may reduce and keep an eye on risk using managed key management, regardless of the size or kind of facility. The automated systems are made to monitor, track, and regulate the distribution of keys to only authorized individuals. A key control system's functionality is improved by having online monitoring, updating, and reporting capabilities, which also add to the integrity of the entire security strategy.

This study was motivated by the fact that Dalhatu Araf Specialist Hospital in Lafia, which serves as a case study, continues to maintain keys manually despite the significant effect of growing internet technologies. As a result, the project seeks to use the bio-informatic and internet-based technologies to automate the hospital's manual key management system and, as a result, add biometric fingerprinting for the signature of office keys. The goal of this work therefore, is to automate the Dalhatu Araf Specialist Hospital in Lafia, Nasarawa State's manual key management system by verifying key collectors' validity using fingerprint biometric authentication, to keep track of the keys that are available and those that are not in relation to the collectors and to stop workers from lying about their arrival time for work.

[*]*Corresponding Author: e-mail: oladunjoye.abbey@yahoo.com*
Tel- +2348026106599
ISSN 2320-7590 (Print) 2583-3863 (Online)

2. Literature Review

Numerous works that are concerned with security and the key management system were been assessed. Design and construction of a door locking security system using GSM were taken into consideration by [5]. The project involved designing and building a remotely operable security door prototype. A GSM phone set functioning as the transmitter and a second GSM phone set with dual-tone multi-frequency (DTMF) linked to the door motor through a DTMF decoder interfaced with a stepper motor and a microcontroller unit. It offers a simple method of operating a lock without making physical touch; however the technology is devoid of a real user authentication mechanism like a biometric or facial recognition system. Additionally, it lacks a notification and alarm system. The dependability of security can be improved by including an additional security element. According to a study by [6] titled "Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone & Computer Set"), a security door can be opened by pressing the designated keys on a mobile phone or by entering the corresponding code into a computer set that is interfaced with the system. When the proper code is entered, the door opens automatically and stays open for 10 seconds before closing again. The security system is inexpensive but is without an automatic code generating and registration mode mechanism. The addition of biometric, auto-generation, and registration mode procedures can be an upgrade.

Design of a "GSM-based Biometric Access Control system" by [7] ensures that, when a finger is put on the scanner, it immediately scans it and compares it to its template. If there is a match, the LCD shows "Access Granted" and the door opens; otherwise, "access refused" is shown. The GSM module sends an Access-Request SMS to the admin phone in the acknowledgement mode with the user's unique 3-digit number, then waits for the admin to acknowledge the request. The microcontroller unlocks the door and shows "access granted" IF the admin agrees to the request. Generally speaking, a biometric system is difficult to hack, but it lacks an automatic option for acknowledgement mode. In a system created by [8], the door is unlocked by the user using an RFID technology. If the erroneous card is inputted, an SMS will be sent to the designated recipient, and the security guard will get notification through a buzzer. The SMS will be delivered via the GSM protocol. A camera would be used for live broadcasting. The system is designed to unlock the locks on the infrastructure's interior doors using the authorized person's cell phone. Although it is a straightforward and reasonably priced security lock system, there is no registration option to enable for the modification of the RFID ID number. To improve security reliability, modification may be done by including an additional security component, such a biometric system.

A microcontroller-based home security system using GSM technology was created by [9]. To control the system, a mobile phone connects through Bluetooth to the microcontroller. Another method for locking or unlocking the system is a manual keypad. Due to its bi-modal (parallel) design, the security system is dependable, but neither the code registration mechanism nor the auto-generated code routine in the microcontroller program are present. The design may be changed to become a multiprotocol device by including devices that create code automatically and serializing the security features. In a security system created by [10], an RFID reader reads the fingerprint from the passive tag and sends it to the microcontroller. If the fingerprint matches, the microcontroller then sends the password to the authenticated prisoner's mobile number, and the authenticated prisoner then enters both the passwords (the one that was already given to the user and the one that was received from the microcontroller) into the keyboard. The locker will be unlocked if the two passwords match, else the microcontroller will send a warning message to the cell phone of the verified prisoner. It is a safe method of managing prisons by utilizing several protocols. The system lacks a registration option that would enable a change in the user's phone number and RFID number without affecting the program. By adding a registration method and enabling code generation rather to utilizing a pre-existing password, the system can be improved.

An intelligent security system for cars was presented by [11], in which the immobilizer and Near Field Communication (NFC) tag are initialized with an authentication key by the manufacturer. A smartphone with NFC capability also has the smart secure mobile application installed by the manufacturer. Using an NFC reader, the vehicle user extracts the authentication key from the NFC tag and saves it in encrypted form. The smartphone is put closer to the immobilizer when it's essential to unlock the car. The immobilizer reads and decrypts the key after placement. The immobilizer then uses an authentication key to verify the key. If they match, it opens the car; if not, it sends a warning message. Using secure hardware, it increases the security of the cars but lacks vehicle location services and a warning system to alert the owner of an intrusion. Combining biometric, GPS, and GSM technology; specifically, using biometric for unlocking, GPS to determine the location of the car, and GSM for notification can increase security.

A "microcontroller-based biometric locker system with short messaging service (SMS)" was created by [2]. The locker is unlocked once the system scans the fingerprint and compares it to the stored pattern. Anytime an unidentified fingerprint is found, the module was able to send a text message using the locker's auto-generated passcode. It is an easy and dependable method of protecting a lock system, but there is no mechanism for registering the new user's finger patterns in the registration mode. Incorporating registration mode and adding more security elements would improve security dependability.

Industrial control systems (ICS) are described as the important component of today's critical infrastructure due to its crucial

function in process control and monitoring, according to [12]'s opinion. Any malfunction or inaccuracy in the system will cause significant harm. The risk of cyber attacks is increased by their accessibility to the internet. As a result, they created an effective key management system (KMS) while retaining the functional aspects of ICS as the foundation for all cryptographic operations. They examined current KMS and their applicability for ICS, after which they offered a brand-new KMS based on Identity Based Cryptography (IBC) as a superior substitute for conventional KMS. The system's use of the key escrow attribute and lack of a revocation mechanism, however, raises certain security concerns. As a method of boosting cyber-security, [13] presented an encrypted control system capable of the dynamic management of the switching of public and private keys. Controller falsification and replay assaults are easy to spot with the control system. Future research will need to evaluate the detection method's efficacy, consider methodical defenses against the attacks' fluctuations in control signals, and create a dynamic mechanism that updates keys appropriately and autonomously using a suitable map in order to avoid storing multiple keys in a control system. An encrypted observer-based control paradigm was put out by [14] to improve cyber security in networked control systems. The suggested paradigm takes use of a semi-homomorphic encryption mechanism, allowing the necessary computation to be performed over encrypted data without the requirement for decryption at the controller and observer levels. The requirements on system parameters to ensure the stability of the closed-loop system, however, provide difficulties for the execution of the suggested technique.

3. Architectural Design of the Developed System

Since the existing system is a conventional system with a manual technique for managing key collection, the designed system automates the manual process of collecting office keys. One must be fully registered in the system's design and have their biometric information recorded. Therefore, before an office key can be granted in conjunction with that specific office number recorded during staff bio-data capture, the employee information is validated as his biometric and registered data during a key collecting event.

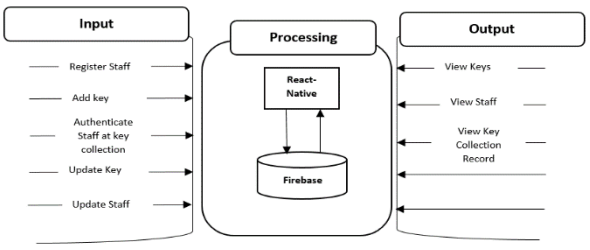

Figure 1. High level model of the developed system

The high-level model in Figure 1 shows the general layout of the automated key management systems that have been created. It depicts the system's input requirements as well as how those requirements are transformed to get the desired results.

The data flow diagrams in Figures 2-5 depict how instruction flows within the developed system.

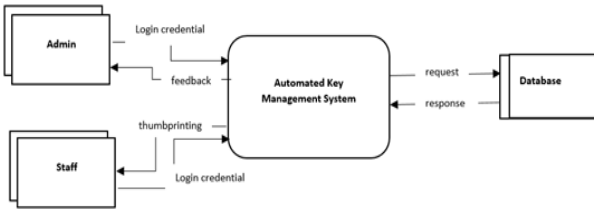

Figure 2. The level-0 data flow diagram depicting the overview of the entire system data flows and storage

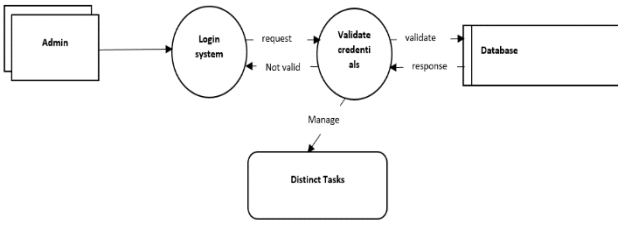

Figure 3. The Level - 1 data flow diagram describing the data flows during the login process.

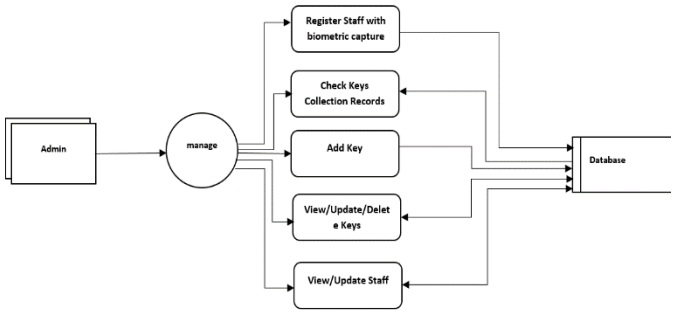

Figure 4. Level 2 - data flow diagram describing the predefined roles of the admin after a successful login to the system

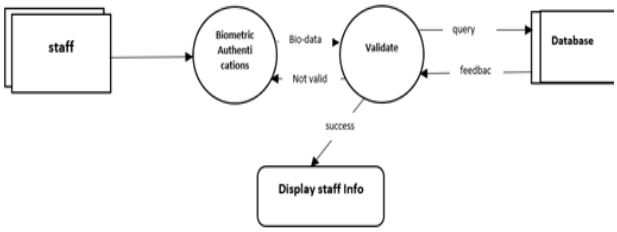

Figure 5. The level 3- data flow diagram in figure describing task of the staff during the collection of an office key.

Figure 6 shows the flowchart of the developed system.

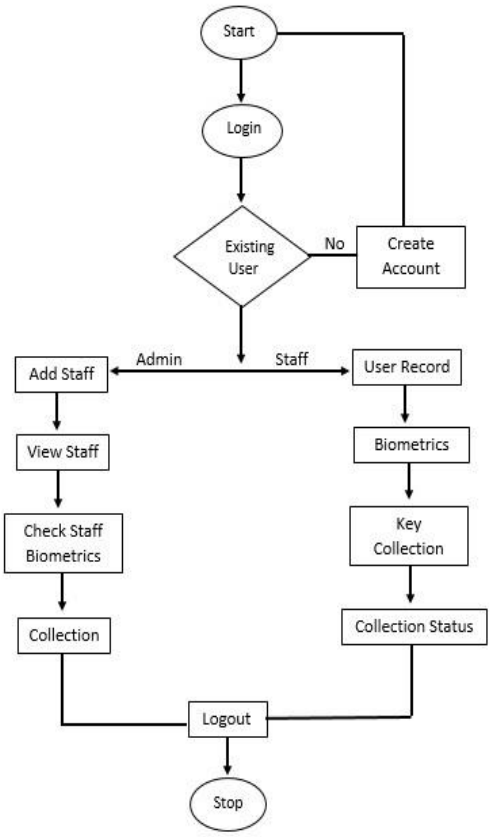

Figure 6. Flowchart of key collection management system

Figure 6 above, shows the process of the application using flow symbols, in which only registered admins can login into the system. If the user has no account then the system asks for the creation of an account first, after which the user can be granted access to the system before accessing its functionalities as shown in the flow diagram.

4. Results and Discussion

The developed system provides a distinct and efficient method for key collections in Dalhatu Araf Specialist Hospital, Lafia. Since the administrator of the developed system employs a biometric technology to check the authenticity of the staff about his or her office, the staff does not have to repeatedly record information during key collections. Key collection records are not at risk from dangers like fire, flood, and vandalism hence, record's longevity is preserved as a result. Personnel impersonation is eliminated since only registered legal staff can be uniquely identified thanks to the use of biometric measures.

The Control/Main Menu as shown in Figure 7 provides an interface for easily navigating hierarchical data. The most common placement of a menu is in the site navigation area or navigation bar and is referred to as a navigation menu**.**

Figure 7. View of the main menu (navigation bar)

- Collect: The collect button is in charge of capturing the data/details of the user at the point of key collection.
- Login: The login page is used by only the admin to access the admin dashboard by which the admin can add staff/user, view staff, and also check collection.

The Key Management System checks the accuracy and also controls the flow of data into the computer. For example, when an admin provides accurate login parameters, the system grants access to its dashboard else it prompts "Wrong Email or Password".

Figure 8 shows the admin successfully login in by taking the admin to its dashboard.

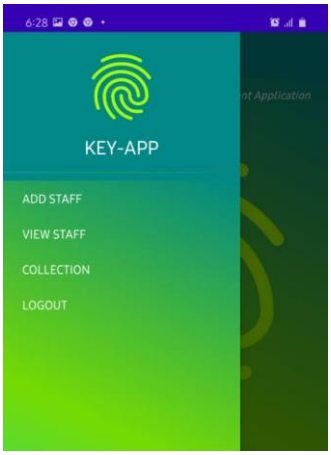

Figure 8. Shows admin dashboard for a successful login

The output from the system accomplish the following objectives:

- Key Collection Record: It displays the list of collection records with their status of either sign-in or sign-out in the key management system as shown in Figure 9.
- Trigger an action: Once a staff collects a key, the system will require the staff to sign-in and the staff will only sign-out at the point of key return.

Figure 9. Shows key record collection.

5. Conclusions

In conclusion, the study optimized the viability offered by android devices with biometric technology to authenticate the staff's genuity during key collection using Java programming language and SQLite database technology after identifying the need for the automation of the manual key collection system and, more importantly, the eradication of staff impersonation in gaining access to staff offices. The development process was streamlined by heavily utilizing the Structured System Analysis and Design approach, which also reduced the cost and work required for deployment. The most important driving force behind this study is the sensitivity and integrity of staff data, hence the established system was created to reduce such hurdles.

This research suggests the following for the intended system's successful and efficient operation:

- The hospital system needs to hold a training session for the personnel in charge of managing the system.
- The admin position, which is charged with recording all personnel data, should go to a hardworking and reliable employee.
- Tablet computers should be used for the application's operations since they allow for a respectable quantity of biometric registration.

References

1. Lia, K, Alfin, NSR., Mada, SWS. and Edi, M., Door-Automation System Using Bluetooth-Based Android for Mobile Phone, *Asian Research Publishing Network (ARPN) Journal of Engineering and Applied Sciences*, Vol. 9 (10), pp 1759-1762, 2014.
2. Crystalynne, DC., Jaswinder, SB., Jocelyn, RH., Ditche, JCA., Melvie, SDC. and Jaira, CI., Development of Microcontroller-Based Biometric Locker System with Short Message Service" *Lecture Notes on Software Engineering*, Vol. 4 (2), pp 103-106, 2016.
3. Moses, T. and Obi, HE., Review on Automobile Crime Prediction Model. *International Journal of Darshan Institute on Engineering Research and Emerging Technologies*, 11(1), 08-13, 2022.
4. Moses, T., Asaju, LB. and Ishaku, WA., An android location-based crime reporting system using the Google Map API. *University of Pitesti Scientific Bulletin: Electronics and Computers Science*, 20 (1), 35-44, 2020.
5. Ushie JO., Donatus EBO., and Akaiso E., Design and Construction of Door Locking Security System Using GSM, *International Journal Of Engineering And Computer Science*, Vol. 2, Issue 7,pp..2235- 2257, 2013.
6. Nwankwo, PN., Nsionu, II. and Ezeilo, CJ., Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone & Computer Set), *Journal of Automation and Control Engineering*, Vol. 1 (1), pp 65-69, 2013.
7. Hussaini, H., Adamu, MZ, Ajagun, AS, Ijemaru, GK. and Oresanya, BO., Design of a GSM-Based Biometric Access Control System, *Control Theory and Informatics*, Vol.4, No 8, pp 1-21, 2014.
8. Jaykrishan, P., Joyson, B., Ketan, P., Viral, P., and Ramanuj, G., Armoured Infrastructure using Multiple Protocols, *International Journal of Computer Science and Information Technology Research*, Vol. 2, No. 4, pp: 170-174, 2014.
9. Hasan, R., Khan, MM., Ashek, A. and Rumpa, IJ., Microcontroller Based Home Security System with GSM Technology, *Open Journal of Safety Science and Technology*, Vol. 5, pp 55-62, 2015.
10. Srinivasan, J. and Krishnamoorthy, M., Implementation of GSM Technology in Prison Locker System, *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, Vol. 12, No. 4, pp 15-18, 2015.
11. Fathima, G., DivyaBarathi, A., Jaya, S., and Manjushree, R., Intelligent Secure System for Vehicles, *International Journal for Scientific Research & Development (IJSRD)*, Vol. 3, No. 02, pp 438-442, 2015.
12. Drias, Z., Serhrouchi, A. and Vogel, O., Identity-based cryptography (IBC) based key management system (KMS) for Industrial Control Systems (ICS), *Cyber*

Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 2017.

13. Kogiso, K., Attack detection and prevention for encrypted control systems by application of switching=key management, *IEEE conference on Decision and Control (CDC)*, Miami, USA, 2018.
14. Sadeghikhorami, L., Zamani, M., Chen, Z. and Safani, A. A., A secure control mechanism for network environments, *Journal of the Franklin Institute,* Vol.357, No. 17, pp. 12264-12280, 2020.

Biographical notes

J. A. Oladunjoye has received his Ph.D. from Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Oyo State, Nigeria. He is the Head of Department, Computer Science, Federal University Wukari, Taraba State and a member of Nigeria Computer Society. His research interest includes Embedded Systems, Big Data Analytics and Digital Signal Processing.

T. Moses has a Ph.D. and is currently a Senior Lecturer at the Department of Computer Science, Federal University Lafia and also a member of Nigeria Computer Society. His research interest includes Distributed Resource Management and Parallel Computation, Distributed Learning.