

Electronic doorbell system using keypad and GSM

O. A. Simon¹, U. I. Bature², K. I. Jahun³, N. M. Tahir⁴

^{1,2,3}Department of Computer and Communications Engineering, Abubakar Tafawa Balewa University Bauchi, Nigeria

⁴Department of Mechatronics and System Engineering, Abubakar Tafawa Balewa University Bauchi, Nigeria

Article Info

Article history:

Received Mar 28, 2020

Revised Apr 21, 2020

Accepted May 10, 2020

Keywords:

Authentication
Electronic doorbell
Home security
Keypad
Security lock

ABSTRACT

In our homes or offices, security has been a vital issue. Control of home security system remotely always offers huge advantages like the arming or disarming of the alarms, video monitoring, and energy management control apart from safeguarding the home free up intruders. Considering the oldest simple methods of security that is the mechanical lock system that has a key as the authentication element, then an upgrade to a universal type, and now unique codes for the lock. The recent advancement in the communication system has brought the tremendous application of communication gadgets into our various areas of life. This work is a real-time smart doorbell notification system for home Security as opposes of the traditional security methods, it is composed of the doorbell interfaced with GSM Module, a GSM module would be triggered to send an SMS to the house owner by pressing the doorbell, the owner will respond to the guest by pressing a button to open the door, otherwise, a message would be displayed to the guest for appropriate action. Then, the keypad is provided for an authorized person for the provision of password for door unlocking, if multiple wrong password attempts were made to unlock, a message of burglary attempt would be sent to the house owner for prompt action. The main benefit of this system is the uniqueness of the incorporation of the password and messaging systems which denies access to any unauthorized personality and owner's awareness method.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

U. I. Bature,
Department of Computer and Communications Engineering,
Abubakar Tafawa Balewa University,
Bauchi, Nigeria.
Email: biusman@atbu.edu.ng

1. INTRODUCTION

A device that is normally positioned near to a building's entrance door that usually indicates the presence of a person when rung is called doorbell, this is a traditional method of alerting the house/building occupant that a visitor or someone is at the entrance. Doorbells were earlier known as a set of clangs [1] usually in mechanical form activated via the pushing/pulling of a cord, in [2] modern doorbells are generally electrical switches. Typically, the phrase is used to refer to a home appliance used at the entrance but there are several applications of the principle of a doorbell system that can be found in many sections of a house or an office. According to [3], in the last several years, doorbells have become an imperative gadget and have been designed to be used for practical visitor-announcement needs, as well as security and safety. As different designers and doorbell manufacturers try to "win" market share, they are constantly adding new features and improving the performance of their different models of doorbells. This has enabled other companies to develop new tools and services which utilize a typical doorbell. Today, security is provided

apace with many doorbells. This has enabled secured properties and lives as well as increasing efficiency and convenient use of doorbells. The need for this efficiency and convenience has resulted in different techniques of using a typical doorbell system.

Cellular network systems are playing an important role in our societies and environment in general. According to the statement in [4], there were more than 2.32 billion smartphone users in 2017 world-wide and these figures would witness an increase to over 2.87 billion in 2020, this indicates the level of patronage for mobile cellular network system and its importance to the entire humanity. This communication system will play an important part in this project. We have been witnessing the benefits of this development long ago, communication systems have used to aid in improving security in various areas. Security in wireless sensor network security approaches was proposed in [5], it was aimed at securing data collection in wireless sensor networks. In 2019, an SMS notification system was proposed [6] to alleviate the cost of information dissemination on the android gadget, another system was proposed [7] that uses telecommunication monitoring system of temperature and humidity via smartphone. In 2019, a survey was conducted to observe and enhance the existing efforts on security systems using cloud platform connected/control via the Wi-Fi system [8]. Optical communication is also another form of communication system, the current passive optical networks are prone to attacks and this can damage how bandwidth fairness mechanism works between the optical network units [9].

Security issues were continuously evolving using communication system as a means for improvement, network on chip (NoC) system was proposed [10], this avoids the stalemate and live lock usually associated with a low area overhead and provides good performance and low latency NoC, also another NoC based system was proposed [11], that offers area optimization apart from the live lock issue. There are a lot of challenges in the security system, cloud-based security challenges and solutions were detailed in [12], and software-defined networks that attempt to provide various security resolutions. The domain technique of non-orthogonal multiple access (NOMA) security issues in cognitive radio inspired networks were proposed [13], the work was able to scheme a tractable analysis structure to estimate the security performance of cooperative NOMA. Mechanical lock systems have been in use long ago as a sole choice for security shield against any burglary attempt. In the 20th century, the biometric system has witnessed its boom, it has been in application in various areas nowadays. A Fingerprint biometric authentication system was proposed [14], the system was able to recognize users' fingerprints, processes and allow access to resources. The demand for new products and services that will make our life more efficient grow just as technology develops. Consider the simple case of lending your apartment key to a friend while you are out of town. This could be made easier by using the security features of this doorbell system as you can easily share your key-lock password with your friend. The history of a doorbell is a long one, starting from the early 19th century and advancing with time. Nowadays, doorbell systems are everywhere, they are used for practical visitor-announcement needs, as well as security and safety. Today, there is a huge variety of wireless and hard-wired options to choose from. Designs range from the purely functional to ornate or sophisticated decorative designs to complement the style of any home or building.

However, an established trend in home securities today involves the use of venerable locking methods and signalling devices that are not capable of sending notifications over long distances. Some of these locking methods include the use of padlocks, Deadbolts, Lever Handle Locks, Knob Locks and some of the signalling devices are chime, bell, or buzzer. These locking methods have helped improve the rate of break-ins in the country. Hitherto, they are geriatric and presents problems. They are extinct which can lead to unlocking problems and eventually damage, also, the loss of the key at crucial moments presents so much inconvenience that could be avoided. In response to this problem, this work proposes the use of a cellular network system to be capable of sending notifications from the doorbell to the owner via text messages. The work also proposes to examine factors that have a positive impact on securing homes and prune the inconveniences the geriatric locking methods present, it will also employ both smart and wireless approaches to doorbell systems to be able to provide an improved system with better security features.

2. RELATED WORK IN THE FIELD OF SECURITY LOCK SYSTEM

The history of the doorbell is stretched back in time, dating from the early 19th century and progressing with time. Today, doorbells are far and wide and are used for practical guest-announcement needs, along with security and safety. Doorbell system plays an important role in our homes and offices, developing projects that address home security and burglary attempts will be a great benefit to the society as the greater demand for doorbell systems today justifies the need for an efficient way to employ the use of a doorbell system, thus, homes and offices will benefit from this improved doorbell system that sends a notification to the house owner via text messages. With the evolvement of smart home technology, the need for smart doorbell greatly increase, it was an integral part of a smart home.

Nowadays security has become the main concern, there is the need for the use of the latest technology in the security monitoring system and a lot of modifications will continue to take place to meet up with the smart home technology requirements of a door lock security system [15]. The existing smart doorbells have been proposed using various methodologies and techniques, like the use of internet-connected based door lock system via Wi-Fi, Bluetooth device, password-based, biometric-based, and Global System for Mobile communication (GSM) based, smart card, Radio Frequency Identification Card (RFID) based, and cloud system for better operation. Various identification and access control security systems were surveyed [16], it shows that various methods of door lock security systems were proposed and more researches were on the way on automatic door lock security system. Near field communication (NFC) was integrated with a smartphone to realized a secure door lock control system [17], it uses a dedicated means of the logical link control protocol (LLCP) exchange along with a timestamp to equal the user's password set of data to verify for access permission or otherwise. Bluetooth based door lock secure system with a low power was proposed [18], the system was also aimed at supporting people with disabilities.

The issues of securing confidential information over the network via the IoT based door security system was proposed using a cryptographically shielded and password-based door lock system [19], a smartphone android app along with cryptographic algorithms and communications gadgets for access denial or granting for authorized persons. Bolt cloud-based device along with Atmega and ESP8266 unit was used for cost-effective and easy install door lock security system [20], the system uses a smartphone with an android app for contact user and the lock system. The use of RFID as an identity card reader, Atmega 16 microcontroller and a keypad is also another form of door lock security system [21] if the identity card reader is true, Atmega permits the entering of a password on the keypad to unlock the door but if a wrong password is entered, the lock stays on. The electronic door lock system for home automation provides dual security by employing a smart card that is easy to use and a keypad lock for added security. The password-based system is another form of security, password system can also be breached or vulnerable to either physical attack or hard to remember password. A 2FYSH based system was proposed [22], which uses two tokens-based verification procedure meant for the replacement of password authentication, the system uses NFC card and mobile phone as the tokens for verification. Another form of securing a system is the One Time Password (OTP) method, it is a potential method for securing a system for possible penetration or unauthorized usage of resources which is valid for one-time authentication [23]. Multi-factor Authentication (MFA) is a security system that probably addresses the issues on passwords, MFA requires three authentication procedures from self-regulating categories authorizations to verify users' IDs: security token (something you have), password (something you know) and biometric authentication (something you are) [24]. Python script algorithm would also be another alternative for implementing an effective security system in detecting human motion [25]. The advantages of this proposed system is the ability to notify owners at any particular point in time when an unauthorized attempt was made to access the system, and it also displays messages in case the owners absent at home to avoid unnecessary time wastage by the quest or visitor.

3. DESIGN METHODOLOGY

3.1. System overview

The proposed system is a smart electronic doorbell system with a keypad security lock and GSM alert. It will serve as a means for providing security to our homes, offices, etc. The work also proposes to examine factors that have a positive impact on securing homes and prune the inconveniences the geriatric locking methods present, this work consists of a microcontroller that will be used to activate a buzzer and send notifications via text messages to the house owner mobile. This door lock system is the keypad lock that allows users to enter a code on a keypad to unlock the lock instead of using a key as shown in a basic design block in Figure 1. It also employs both smart and wireless approaches to doorbell systems to be able to provide an improved system with better security features.

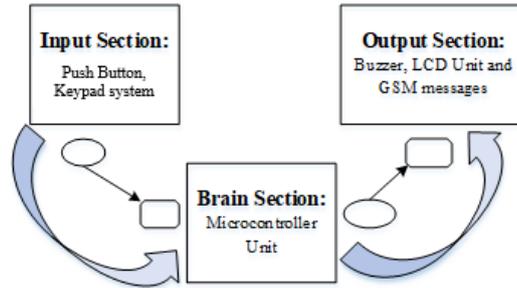


Figure 1. Basic block of the system

3.2. System block design

There are many methods of designing an electronic doorbell system but all these methodologies require human assistance, in this work GSM alert and keypad security device were added in other to unlock the door and alert the user without human intervention. The system will be designed to carefully send signals to the user in real-time. The overall design was broken into function block diagrams where each block in the diagram represent a section of the circuit that carries out a specific function, several steps taken in developing this work are stated thus:

- Understanding the problem and gathering information.
- Choosing the appropriate method with a minimum cost that will be used in solving the problem based on the information gathered.
- Selection of design tools and sourcing of components.
- Hardware construction and testing.
- Software design and testing.
- Software and hardware integration and final testing.

This work is developed to ensure a higher speed of communication and monitoring, the major components used in the work design are Atmega microcontroller, GSM module, keypad and liquid crystal display. The block diagram is shown in Figure 2.

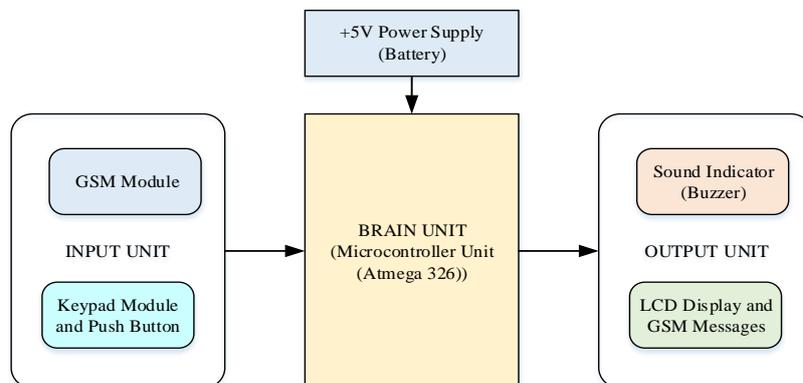


Figure 2. Block diagram of the system

3.3. Flowchart

The proposed flow chart diagram of the system is shown in Figure 3. Section 1; The Guest will push the push button to pronounce his presence, the owner will be notified via the buzzer inside the house, if there is a response, the door will be open for the guest otherwise a message will be displayed on the LCD for the guest to know the status of the owner (at home or not) after the owner received an SMS alert that he has a visitor at home. Section 2; for the authorized person who has a valid password, the user will input password, is password correct? The system will check for the password authenticity if valid the door will open otherwise the door remains close, after three unsuccessful trials, the system will send a burglary attempt message to the owner.

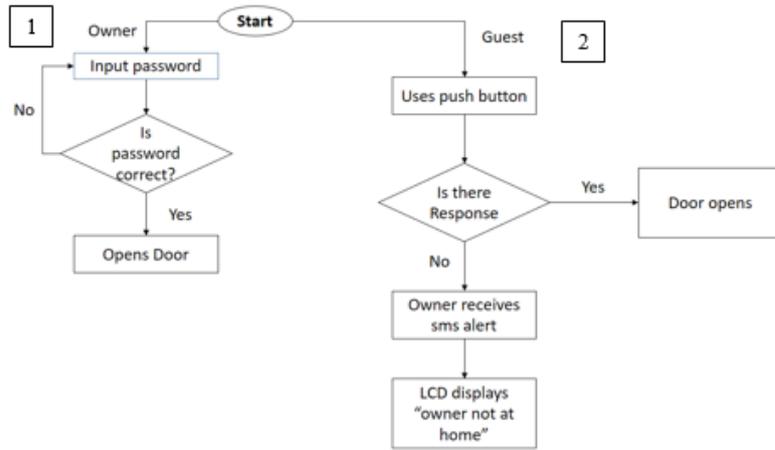


Figure 3. The Flowchart of the system

4. DISCUSSION

The design and implementation of an electronic doorbell system with a keypad security lock and GSM alert are primarily used for signalling (doorbell) and security (door lock) purposes. This doorbell system also ensures that the house owner get notifications in the form of text messages (SMS) from the system after certain conditions are met.

4.1. Working principles

This work consists of some numbers of modules as shown in the block diagram in Figure 2 and Figure 4 as the circuit diagram, the operation of each of these modules is described below;

- Power supply to provide power for the different components of the work at all times.
- A push-button to be used by a visitor.
- An LCD to display greetings and other information for the visitor.
- A keypad outside the door to unlock the house using a password.
- A buzzer to alert the house owner of the presence of a visitor at the door.
- A button to unlock the door from inside the house.
- A GSM module to send a message to the house owner if wrong attempts are made to unlock the house using the keypad.

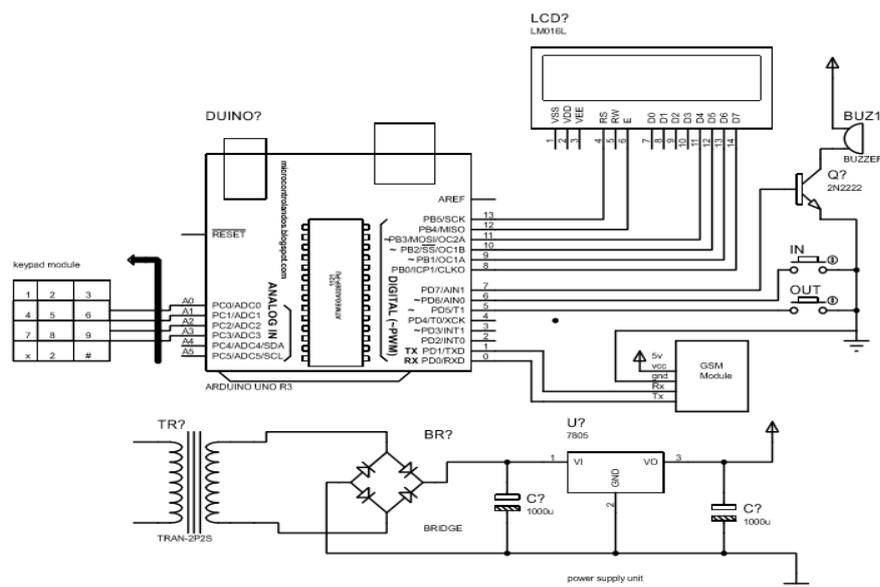


Figure 4. The system circuit diagram

The push-button is designed to be placed outside the door so visitors can come and use to ring a bell inside the house as well as an LCD to display messages for visitors. When the doorbell button is pushed, a bell is activated inside the house and the LCD 'Bell Ringing', if the owner should respond by opening the door, the LCD 'Welcome' and the door is opened; however, after three attempts of ringing the bell without getting a response from inside the house, the system sends an SMS to the house owner to alert him/her of a possible guest at the door and the LCD 'Owner not at home'. The keypad is designed to unlock the house door from outside the door, it is placed closed to the door so that the house owner can input the correct password and open the house door. However, if multiple wrong attempts were made to unlock the door using the keypad, the system sends an SMS to the house owner to alert him/her of a possible burglary attempt.

4.2. Casing

The casing refers to the external housing of the project. The casing used for this work is fabricated using plastic sheets for making the outer housing for the project. The casing for the work can be illustrated by the work photography illustrated in Figure 5. The display unit of LCD, the keypad unit for inputting the registered password, push-button for the buzzer alert, and entrance door were shown in the figure.



Figure 5. Pictorial view of the completed work case

4.3. GSM module test

A simple code was used to test that the GSM module could send SMS to the owner's mobile phone. The code is shown in Figure 6.

```

// GSM Module SMS Sending Tests
void setup()
{
  Serial.begin(9600); //Initialise serial to communicate with GSM Modem
}

void loop()
{
  delay(10000); //Give enough time for GSM to register on Network
  SendSMS(); //Send one SMS
  while(1); //Wait forever
}

void SendSMS()
{
  Serial.println("AT+CMGF=1"); //To send SMS in Text Mode
  delay(1000);
  Serial.println("AT+CMGS=\"+9198xxxxxxx\""); //Change to destination phone number
  delay(1000);
  Serial.println("Hello from GSM Modem!"); //the content of the message
  delay(200);
  Serial.println((char)26); //the stopping character Ctrl+Z
  delay(1000);
}

```

Figure 6. GSM messages testing codes

To complete the test, these steps were followed:

- A Subscriber Identification Module (SIM) card was inserted into the modem.
- After uploading the system was powered off and transmitter and receiver lines were connected.
- Both Atmega and GSM Modem were turned ON
- After a few seconds, the network LED blinking slows down. This implies that the modem is registered on the network.
- After 15 Seconds an SMS was received. NOTE: If it takes too long to register on the network the 10 Second delay is increased to a larger value.

4.4. Access granted process

This section is executed after a successful password login, the “Access Granted” means allow access to the user after password successful verification, and the buzzer will notify the house owner that someone is accessing the door system. The “WELCOME” is a message that will be displayed on the screen to the visitor, and “false” means access is denied if a wrong password is provided. The Atmega codes for the door entrance are shown in Figure 7.

Figure 8 shows the system process of access granted, after a successful password authentication the system will grant access to the entrance door and will also display “Access Granted” on the LCD as shown in the figure. But, if a wrong password was entered three times, the system will not only be denied access to the entrance but also send messages to the owner’s mobile phone indicating that an attempt was made to access the door entrance.

```

if (access) {
  lcd.clear();
  lcd.print("Access Granted");
  myservo.write(90);
  digitalWrite(buzzer, HIGH);
  delay(500);
  digitalWrite(buzzer, LOW);
  delay(5000);
  myservo.write(0);
  lcd.clear();
  lcd.print("WELCOME");
  access = false;
  x = 1;
  y = 1;
}

```

Figure 7. Codes for the door entrance



Figure 8. System access granted process

5. CONCLUSION

The Doorbell system is widely in use today, more are been produced daily with different modifications thus there is a high demand for the doorbells with the best features. This work incorporates a doorbell, a lock system, and a display system to carry out the functions discussed before now. However, there are some limitations to this implementation as it lacks the necessary security features to verify the identity of the visitor before letting him/her into the house.

ACKNOWLEDGEMENTS

This work was conducted at the DCCE Laboratory of Computer and Communications Engineering Department, Abubakar Tafawa Balewa University Bauchi (ATBU), Nigeria. Our profound gratitude goes to the Head of the department and members of the Lab for their overwhelming effort and support towards the successful completion of this project.

REFERENCES

- [1] White, L.N. and White, E.B., Marietta. Arcadia Publishing. pp. 34- ISBN 978-0-7385-3231-8. Retrieved 24 March, 2020, 2004.
- [2] Sanchez, Marla C., Koomey, Jonathan G., Moezzi, Mithra M., Meier, Alan, & Huber, Wolfgang, Miscellaneous electricity use in U.S. homes. United States. <http://www.osti.gov/bridge/servlets/purl/795945-9c8LM1/native/795945.pdf>, 1999.
- [3] Muktar, Ahmed, AbdulAziz Ahmed, and Ahmed Salad, "A Framework for Ultrasonic Doorbell System with Object Detection." *Somali Journal of Engineering and Science*, vol. 2, no. 1, pp. 1-6, 2017.
- [4] Cha, S.S. and Seo, B.K., "Smartphone use and smartphone addiction in middle school students in Korea: Prevalence, social networking service, and game use," *Health psychology open*, vol. 5, no. 1, 2018.
- [5] B. Abidi, A. Jilbab, M. El Haziti, "Security in wireless sensor networks," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no. 1, pp. 13-18, 2019.
- [6] Heryati, A., Yulianti, E., Sartika, D., Saluza, I. and Sanmorino, A., "The design of smart notification on android gadget for academic announcement." *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 1, pp.147-152, 2019.
- [7] Panjaitan, S.D., Fratama, N., Hartoyo, A. and Kurnianto, R., "Telemonitoring Temperature and Humidity at Bio-energy Process using Smart Phones." *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 14, no. 2, pp.762, 2016.
- [8] C. R. Balamurugan, P. Vijayakumar, "Cloud connected smart home gas cylinder platform based wifi control," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 8, no. 3, pp. 117-121, 2019.
- [9] Atan, F.M., Zulkifli, N., Idrus, S.M., Ismail, N.A. and Zin, A.M., "Impact of security breach on the upstream delay performance of next generation gigabit passive optical networks." *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 3, pp.1053-1058, 2019.
- [10] Kendaganna, S.S., Jatti, A. and Uma, B.V., "Design and implementation of secured agent based NoC using shortest path routing algorithm." *International Journal of Electrical and Computer Engineering*, vol. 9, no. 2, pp. 950, 2019.
- [11] Swamy, S., Jatti, A. and BV, U., "Reconfigurable High Performance Secured NoC Design Using Hierarchical Agent-based Monitoring System." *International Journal of Electrical & Computer Engineering*, vol. 6, no. 8, pp. 4164-4174, 2018.
- [12] Hassan, W., Chou, T.S., Li, X., Appiah-Kubi, P. and Tamer, O., "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks." *International Journal of Informatics and Communication Technology (IJ-ICT)*, Vol.8, No.3, pp. 162~183, 2019.
- [13] Hoang, T.A., Le, C.B. and Do, D.T., "Security performance analysis for power domain NOMA employing in cognitive radio networks." *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp.1046-1054, 2020.
- [14] Martin, M., Štefan, K. and L'ubor, F., "Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino." *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 16, no. 2, pp.755-765, 2018.
- [15] Nehete, P.R., Chaudhari, J.P., Pachpande, S.R. and Rane, K.P., "Literature survey on door lock security systems." *International Journal of Computer Applications*, vol. 153, no. 2, pp.13-18, 2016.
- [16] Divya, R.S. and Mathew, M., "April. Survey on various door lock access control mechanisms." In *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, IEEE, pp. 1-3, 2017.
- [17] Hung, C.H., Bai, Y.W. and Ren, J.H., "June. Design and implementation of a door lock control based on a near field communication of a smartphone." In *2015 IEEE International Conference on Consumer Electronics-Taiwan*, IEEE, pp. 45-46, 2015.
- [18] Hadis, M.S., Palantei, E., Ilham, A.A. and Hendra, A., "Design of smart lock system for doors with special features using bluetooth technology." In *2018 International Conference on Information and Communications Technology (ICOIACT)*, IEEE, pp. 396-400, 2018.

- [19] Ahtsham, M., Yan, H.Y. and Ali, U., "IoT Based Door Lock Surveillance System Using Cryptographic Algorithms". In *2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC)*, IEEE, pp. 448-453, 2019.
- [20] Patil, A.V., Akshay, S., Patgar, C., Prakash, S. and AJ, S.K., "Android Based Smart Door Locking System." *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 01, pp. 329-331, 2020.
- [21] S. Mohammed and A. H. Alkeelani, "Locker Security System Using Keypad and RFID," *2019 International Conference of Computer Science and Renewable Energies (ICCSRE)*, Agadir, Morocco, pp. 1-5, 2019.
- [22] Pranata, S. and Nugroho, H.T., "2FYSH: two-factor authentication you should have for password replacement". *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 2, pp.693-702, 2019.
- [23] Prasetyo, B.H., et al., "One-Time Password Implementation on Lego Mindstorms NXT," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 12, no. 3, pp. 689-694, 2014.
- [24] D Dasgupta, A Roy, "A Nag. Multi-Factor Authentication. Advances in User Authentication". Cham: Springer *International Publishing*. pp.185–233, 2017.
- [25] Z. G. Faisal, M. S. Hussein, A. M. Abood, "Design and realization of motion detector system for house security," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 6, pp. 3211-3217, 2019.

BIOGRAPHIES OF AUTHORS



O. A. Simon is a First-degree holder in computer and communications engineering (B.Eng.) from the Department of Computer and Communications Engineering, Abubakar Tafawa Balewa University Bauchi (ATBU), Nigeria. He's focus is on embedded systems and microelectronic system.



U. I. Bature is currently a PhD. Candidate in the Department of Electrical Engineering, Universiti of Teknologi Petronas (UTP) Malaysia. He received a B.Eng. Computer Engineering from Bayero University Kano (BUK), Kano city, Nigeria and degree of Master of Engineering (Electrical - Computer and Microelectronic system) from Universiti Teknologi Malaysia (UTM), Skudai, Johor Bahru, Malaysia. He is currently a lecturer in the Department of Computer and Communications Engineering, Abubakar Tafawa Balewa University Bauchi (ATBU), Nigeria. His research interest includes Image processing, Nano-material design, embedded systems and Biomedical Systems



K. I. Jahun received a B. Eng. Electrical and Electronics Engineering from Federal University of Technology, Yola Adamawa state, Nigeria. M. Eng. (Communication Engineering) from Universiti Tun Hussein Onn Malaysia, Parit Raja Johor Malaysia. Currently a Lecturer in Department of Computer and Communications Engineering, Abubakar Tafawa Balewa University, Bauchi, Nigeria. His research interest includes communication systems, Microwave, Antenna and Propagation.



N. M. Tahir received the B.Eng. degree in Electrical Engineering from Bayero University, Kano in 2012 and M. Eng. Degree in Mechatronics and Automatic Control from the Universiti Teknologi Malaysia in 2016. He has been involved in research at Mechatronics systems and Robotics Laboratory in Universiti Teknologi Malaysia on vibration control, robotics and Mechatronics system design. He has been a lecturer at the Department of mechatronic and system Engineering, Abubakar Tafawa Balewa University, Bauchi Nigeria since 2014. His main research interests include Vibration Control, Mechatronics Systems Design, Control System Design and Robotics.