A Prototype Model of an IoT-based Door System using Double-access Fingerprint Technique

C. O. Akanbi[1*], I. K. Ogundoyin[1], J. O. Akintola[2], K. Ameenah[1]

[1]Department of Information and Communication Technology, Osun State University, Osogbo, Nigeria.
[2]Department of Electrical and Electronic Engineering, Osun State University, Osogbo, Nigeria.

ABSTRACT: Security of lives and properties remains a trending issue of optimal concern in the recent times. It is one of the major issues posing challenges to governments, establishments and individuals. Common security techniques such as the use of keys, passwords and cards are used in home environments and hotels for traditional authentication. Others include lock codes, mechanical doors or electronics RFID Card Door. However, compromise of these security techniques such as property theft and unauthorized entry by visitors and hotel staff is due to a single authenticated access method which is not trustworthy and reliable. This calls for an improved technique. An IoT-based Smart Door System Model that provide double access authentication through fingerprint modules is presented for hotel and guest houses in this paper. The proposed system architecture design specifies all the modules involved and the circuit diagram designed specifies various modules inter connectivity. The prototype implementation software developed in C programming language was tested with several series of captured templates. The prototype test conducted showed that the Smart door system developed responded only to fingerprint signature and unlocks the door when it matches with signatures captured during booking.

. ***KEYWORDS:*** Arduino, biometry, fingerprint, sensor, smart door, IoT

[Received May 16, 2019, Revised March 24, 2020, Accepted April 6, 2020] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

Security of lives and properties remains a trending issue of optimal concern in the recent times. It is one of the major issues posing challenges to Governments, Establishments and Individuals. As a matter of necessity, people are becoming increasingly conscious and more alert to security issues. Doors are known to prevent possible invasion to rooms or buildings in order to ensure safety. Therefore, importance of door system in ensuring security and privacy cannot be over emphasized (Falohun *et.al*,, 2012; Aii, 2002). A security door system has the ability to secure and control access into the building by enforcing authentication. Different traditional and common authentication methods adopted in home environments, which include the use of cards, keys, and passwords were presented in (Aru, 2013; Tolga and Huseyin, 2015).

Others include lock codes, mechanical doors or even electronic RFID cards, biometrics etc. Biometric method identifies or authenticate user using any of series of users behavioral or physical features instead of codes or key. These features include retina scans palm or hand geometry, fingerprints, and iris scans, writing or signature style, facial mapping, and more recently, maps of users' DNA (Woodward and Higgin 2003; Zorzi *et.al.*, 2010). The major limitation of this method is that it has a single authentication right. As a result, it can be easily compromised in terms of room property theft by unauthorized persons posing as visitors or hotel staff. This has proven the existing methods to be less reliable and call for an improved, more secured, trusted and coordinated means of securing homes particularly gates and doors within buildings (Falohun *et.al*., 2012; Mohd, 2005).

New technologies such as The Internet of things (IoT) which is a networked system for validating, controlling and monitoring the security has been identified to provide solution to the above single access problem. IoT is the inter-networking of physical devices to provide network connectivity of various devices and exchange of data and information automatically through internet from anywhere around the world (Zorzi,2010). With IoT multi access technology, the access right to doors could also be remotely given or withdrawn. The security system attached to the door will allow or deny access to the room by capturing user's fingerprint which cannot be borrowed, stolen, forgotten or compromised. This makes it practically impossible for unauthorized users to access rooms (Aru, 2013, Wildes, 1997).

This paper presents a double authentication IoT security door technique which uses fingerprint technology to provide a well secured and access to both the users and the administrators in homes and hotels. The advantage that this has over other common security doors is the ease of changing access rights to the door whenever a client tenancy expires in a room and facilitates booking online and controlling your door lock during your tenancy periods.

*Corresponding author: akanbico@uniosun.edu.ng
doi: http://dx.doi.org/10.4314/njtd.v17i2.10

II. RELATED WORKS

Several biometric technologies have been identified in security door systems (Jain, Flynn and Ross, 2007; Pankanti Prebhakar and Jain, 2002). The fingerprint technology utilizes human fingerprint templates to recognize him through corresponding scanning device and this technology is not only employed in area of security, but also in forensic or crime investigations. The major limitations of fingerprint technology could be false acceptance or false rejection of individuals fingerprint due to aging and medical conditions of an individual which may hinder capturing by the fingerprint scanner. A fingerprint authentication system mainly comprises the (i) Sensor device for acquisition of biometric raw data (ii) Feature extraction for template creation (iii) Matcher to compare the actual biometric template with the stored reference templates and (iv) Reference archive for storing the biometric reference templates.

In the view of Nehete (2016), Door lock security systems are classified based on technology used as (i) Password based, (ii) Biometric based, (iii) GSM based, (iv) smart card based, (v) RFID based, (vi) Door phone based, (vii) Bluetooth based, (vii) Social networking sites based, (viii) OTP based, (ix) Motion detector based, (x) VB based, (xi) Combined system. Some of these are reviewed in this paper.

Fredrick (2014) presented attendance management system that uses fingerprint technology. The developed system implanted in a fingerprint acknowledgment/verification system that is based on minutiae points. Extracts of the local characteristic (minutiae points template) of a fingerprint was used. Matching was carried out during verification and registration stage and match percentage determine success or failure of the process. The technique presented also record time-in and time-out of workers and students. This feature assists in proper time management of lecturers and students and also use of paper in generating timely report. The limitation of this technique is that it uses a single authenticated access method which is not trustworthy and reliable.

Shoewu, Olaniyi and Lawson (2011) explore the concept of Biometric Fingerprint and Iris Recognition Technology for smart homes. Multi-biometrics system was employed to enforce reliability. Users fingerprints and iris data was captured and a processed generated template was stored in the database. During authentication, Fingerprint Recognition Technology (FRT) and Iris Recognition Technology (IRT) accept and compare the supplied biometric data with the database contents. Any mismatch in the data will leads to failed authorization. Despite the multiple security level, inability of users with disability remain it major drawback.

Burak, Tolga, and Huseyin (2015) present Real Time Smart Door System for Home Security. The system makes use of the development of video technology and Raspberry Pi as a security and safety tool in identifying and visualizing people who visit the home. The study uses two different technologies (Video and Smart Phone). The video was used to watch the front door in real time while the phone server as voice communication tool. The system presented in the study offers user several benefits which include having knowledge of visitors without accessing the door, streaming of activities behind the door and so on. Cost of real-life implementation remains the drawback of the system.

Hitachi (2004) worked on finger-vein-authentication as a method to ensure security to life and property. Two applications were demonstrated for door-access control. The techniques require users who want to access the door to have identity number. Finger-vein details are verified and authorization takes place. The system server tracks records of incoming and outgoing users. Convenience of use is a question for uneducated users.

Akhtar (2016) presents an IoT based autonomous alarm and access control system that can automatically switch on the alarm system when the last person leaves the premises. The solution is a combination of hardware and software components; distributed alarm and access control modules, mobile App and a central server with database connecting every object in the system together. The alarm and access control modules are deployed in each room where they operate independently with other modules in the system. These modules can automatically arm and disarm their room alarm system based on occupancy and along with that they control access to the entry points of the room. The prototype was installed in one of the office room of Adeo OS Apps for testing and evaluation purpose.

Djupsjo and Almosawi, (2018) developed of an IoT application based upon digitizing a smart door lock for making it connected to the internet and able to recognize employees that work in the office. Particle Photon Microcontroller was employed as the Microcontroller in their work to handle both WiFi and Bluetooth communication in a test environment proposed. The architectural plans are selected for the developed and Android-based Application. Detailed explanation made up of multi-master database (Azure active directory) using a new technique called Eddystone which serves as the transmission protocol with Bluetooth beacons. The Android application developed delivered a secure flowing and functional IoT system. Although, the system exhibits high cohesion among its component, it ability to use an alternative workflow is low which can leads to unresponsiveness if missing error callbacks occur. Also, the system control is restricted and can only function maximally within limited coverage of Wifi and Bluetooth. Complete reliance on password and token as credential for authentication could be easily compromised compare with biometric authentication adopted in this research work.

Though, some of the above papers reviewed are connected to this study in terms of biometric technology authentication and IoT but none of the works has combined the two technologies together. This work explored the two technologies an IoT enabled based door system for a reliable

double-access authentication in hotels and other establishments.

III. SYSTEM DESIGN AND IMPLEMENTATION

Software engineering approach adopted for the design and implementation in this work is prototyping. This is due to the high cost of real-life implementation in an hotel environment. So, a small casing (box) with a front door was constructed to depict a door which has solenoid lock and finger print sensor.

A. System Design

The schematic diagram for the proposed architecture is shown in Figure 1. The hotel reception has fingerprint module, an Arduino with Ethernet Shield and a computer. Also, at the entrance of the door, there is a fingerprint module. The prototype door is opened only when the fingerprint frames captured during the booking at the hotel reception or during online registration matches with the one captured at the entrance of the door.

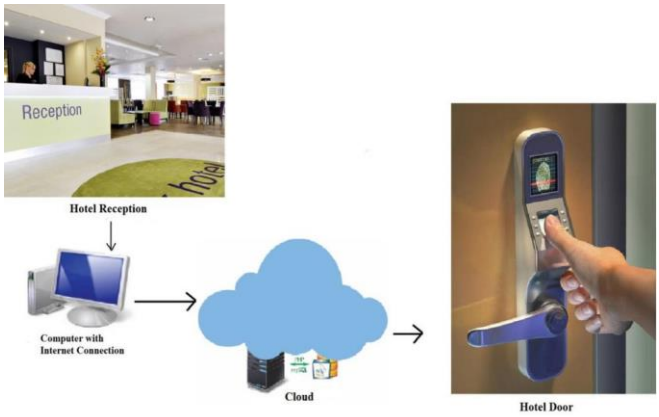

Figure 1: Schematic diagram of the iot controlled smart door system.

Also the block diagram in Figure 2 shows the system architecture of the proposed system consisting of six components which are Fingerprint Sensors, Relay module, Web Server, Arduino with ethernet shield, Solenoid lock and Laptop PC. This architecture defines how different components exchange data through the interaction of web service.

1.) Fingerprint sensor module

A fingerprint sensor module is a device used electronically to capture a digital image of the fingerprint pattern. This is essential in the design to store, compare and match fingerprints. The captured image (live scan) is used to generate a template (a collection of features extracted from user) which is used for digital authentication. This sensor has in-built ROM, Digital Signal Processor (DSP) and RAM. The biometric fingerprint sensor serves as the main device for the verification of fingerprints and it has a DSP controller for easy integration with an Arduino pin. The Optical fingerprint sensors convert light incident energy on the detector into

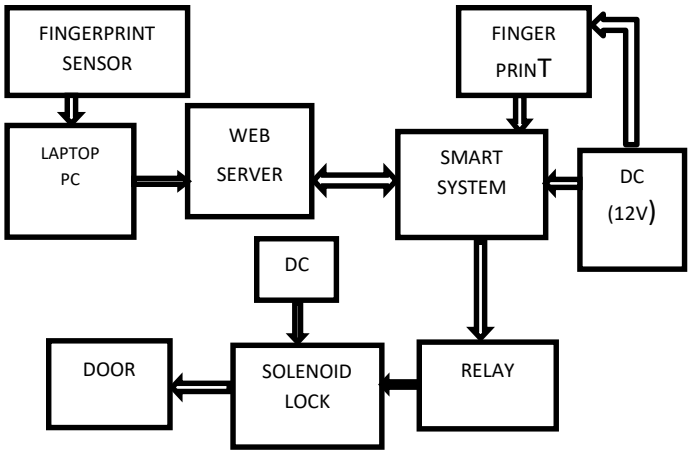

Figure 2: Block diagram of the proposed system.

electrical charge using arrays of phototransistor detectors. Also, the sensor package is capable of illuminating the finger due to the presence of light-emitting-diode (LED). With optical sensors, LED light sources illuminates fingers when placed on the plate. The image is projected on a CMOS image sensor through a prism and a system of lenses. Using frame grabber techniques, the image is stored and ready for analysis. Two fingerprint sensors are employed in this proposed system, one was attached to the laptop (placed at the hotel reception room) to register customers 's fingerprint, generates templates of the user's print in binary form and stored on the server database with a unique id and the other was attached to each room door allocated. To grant access to the room, a customer's thumbprints on the door fingerprint module. If a match is found in the database, access to the room is allowed, otherwise access is denied.

2.) Arduino

Arduino is an open-source platform used for building electronics projects. It has a board (microcontroller) that is programmable through an Integrated Development Environment (IDE) that runs on computer. The Microcontroller on the Arduino Board is not the same with that of microprocessors used in personal computers. It is purposely designed to be embedded in other applications. Micro controller is used to automatically control products and devices. In this research work, it is used to get instruction from the fingerprint sensor, send the instruction gotten to the Arduino ethernet shield and receive response from the ethernet shield.

3.) Arduino ethernet shield

The Arduino Ethernet Shield connects Arduino to the internet. This module which is plugged onto the Arduino Board connects it to the network using an RJ-45 cable. It covers the configurations of communication details between the Arduino Ethernet shield and the server. The Ethernet shield is connected through the internet to the web server. In this paper, Ethernet shield acts as a client, once Ethernet shield receives a template from the microcontroller, it requests for the fingerprint template in the web server, if match is found, the server sends to the Ethernet shield.

4.) Relay module and solenoid lock

The relay module is used for triggering the state of a component in the device which waits for the Arduino to send a signal to the relay to activate a component. This module triggers the solenoid. Solenoid lock is used in a variety of applications, from electronic hobbies to appliances. Most commonly, they are found in applications that require an automatic on/off feature, like an electric lock or latch. It is used in this project to control the opening and closing of the prototype door.

5.) Web server

In this paper, a web page is designed using HTML5 and PHP. The fingerprint templates generated, pasted and saved on the webserver. Webserver uses HTTP (Hypertext Transfer Protocol) to save files that form web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.

6.) Laptop

This is placed in a hotel reception room for hotel administration and customers booking. The web page for registration is launched using any web browser, and then the finger prints (256 bytes data) of the new user are also submitted as part of the online form. In the web server the web script handling the forms, automatically logs the record and returns all the finger prints upon request by the door Smart System through Arduino Ethernet. This in turn unlocks the solenoid lock if a match is found in the database.

B. Prototype Model Design

A prototype door system and other modules are shown in Figure 2 and Figure 3. The prototype design consists of the fingerprint module, an Arduino with Ethernet Shield module all networked to a computer system in the hotel reception office for booking. Also, at each door entrance, we have fingerprint module attached for capturing fingerprint of the customers earlier allocated to a room by the receptionist. The captured data are logged on to the database online. Access to the room is given only to the authentic person whose fingerprint captured at the allotted room door matches with fingerprint captured at the reception/booking office point. In this design there is a seamless integration between Hotel reception and the rooms. This system runs on both internet and local area network available in the Hotel.

C. Circuit Model Design

The prototype circuit diagram is as shown in Figure 5. It is made up of a capacitive LLC751 fingerprint sensor, which is designed to work with +5 V DC. It is made up an array capacitor plates to image the fingerprint. Skin is conductive enough to provide a capacitive coupling with an individual capacitive element on the array using differences between skin-sensor and air-sensor contact in terms of capacitive values. When a finger is placed on the sensor, an array of pixels measures the variation in capacity between the valleys and the ridges in the finger surface of an individual. LLC751 which is the most used/interfaced fingerprint with a microcontroller or Arduino is adopted for this prototype design.

Figure 3: Prototype door system.

Figure 4: Components attached to the door system.

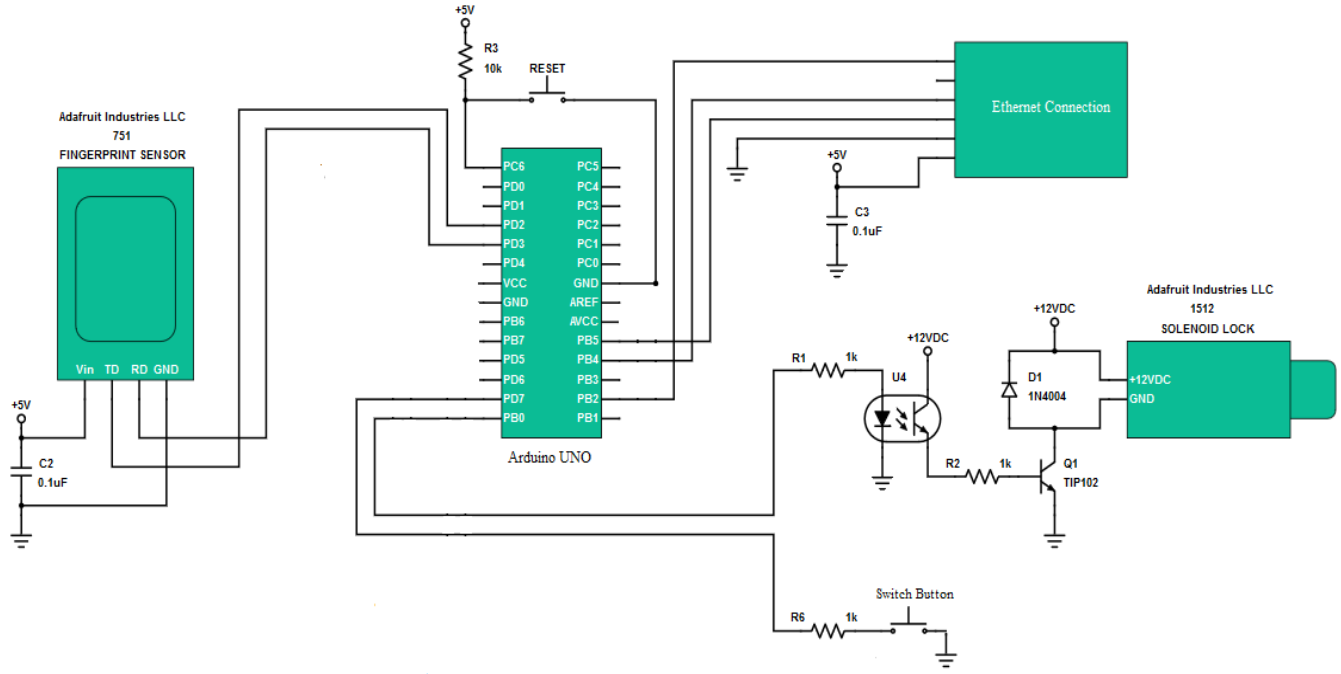

Figure 5: Prototype system model circuit diagram.

As shown in circuit diagram of Figure 5, the Arduino stands between all the peripheral components and controls them based on the logic programmed in it. A simple explanation of the logic programmed into the Ardunio is that anytime pin 4 which is connected to TD on the fingerprint goes high, which means a positive signal is sent from the fingerprint module immediately a print match occurs on any finger placed on the module. The "Open Door" class is called, which send a +5 V to actuate solenoid lock. Otherwise when a negative signal is sent from the fingerprint module immediately a print mismatch occurs on any finger placed on the module, the "GetPrintFromInternet" class is called, which first confirms that the Ethernet module has internet, the pings the web address programmed to return registered print for the specific door.

The http header message is returned when the print message is invoked through fingerprint module. Then in the GetPrintFormInternet class, the 256 bytes data which is received as a string, is looped through and turned to an array. This array is then saved to the fingerprint module and the "Checkprint" class is called when the new user places a finger for the second time. This activity enables the system to get the latest print stored on the server. Technically, the system was designed this way to make sure that the Ethernet module is only used to get a new print when a mismatch occurs. However, intelligence was put into this in that it adds 1 minute to the time of retry (i.e. to the delay time before recalling the "GetPrintFormInternet" class) so as to avoid system overload due to several trials, considering low memory of an Arduino. The circuit diagram also shows the solenoid lock powered by +12Vdc, it also shares the same ground with the system but separated by an amplifier to avoid sending +12Vdc to the other part of the system.

D. Implementation

Hardware, Software, Data storage and Communication links were the major components. As shown in the Figure 5, Tx-out and Rx-in of the LLC751 fingerprint sensor are connected to the pin 7 and pin 6 of the Arduino connected to the laptop for registering fingerprints and assigning the ID to the prints. Through this, the fingerprint templates (in binary form) is captured on the webpage and user's details are entered and stored on the web server which guarantee access to a room in the hotel while booking. Tx-out and Rx-in of the second sensor are connected to the pin 8 and pin 9 of the second Arduino respectively. The solenoid lock was connected to one of the output ports of the Arduino. Making a network with the relay allows switching between the 5V and the 12V electrical components.

The Arduino together with Arduino Ethernet shield were connected to the prototype door and the power adaptor is turned on. When power adaptor is on, the system boots up the fingerprint sensor and waits for a print, once a user thumbprint the microcontroller at the Arduino get instruction from the sensor in digital format. The microcontroller sends the instruction through arithmetic and logic unit to the Ethernet shield. Then the Ethernet shield (client) also request from the server if the template just captured matches with any of the template in the webserver, if match found the server send to the Ethernet shield and from the Ethernet shield to the microcontroller. The microcontroller now send high signal to the relay to actuate the solenoid lock (the relay triggers the solenoid lock because the power coming from the microcontroller is too low for the solenoid lock) when the relay has been actuated it make a small sound and the door open (access granted) for 5seconds (the time has been programmed) and close afterwards. If no match is found, the system will not take any action at all. The system works very

fast so when someone places a finger, it will respond instantly if the prints match. The Arduino integrates all the different modules and make the system function, since it uses all parts of the different modules for it to function properly. C code developed for this prototype program in the Arduino IDE is depicted in Appendix I.

Three actions are possible on the fingerprint module itself, which are storage, comparison, memory check, image (prints) retrieval and prints deletion. The working methodology however adopted is the exact way the fingerprint actually compares any finger placed on it with the stored finger. The fingerprint module stores a 562 bytes data on a unique memory location for each finger print stored. The very fast process of converting the finger image (print) scanned to the 562 bytes data is done each time a finger is placed on it for access. The bytes data of the current finger being checked against the ones on the database is stored in a buffer in the Arduino. This process retrieves the exact image data after registration, and store image data on a SQL database through a form written in php as seen in the code in Appendix I.

The system at the door checks for a new print only if a wrong finger is placed on it. It does this by first checking the internet connectivity, if available if does pinging of the IP address of the server, if available it goes on to call the address using http call. The specific address called is a php file, written to query the sql database for the latest print details stored with a door number equal to the id sent, if any row is available with this details it sends the 652 bytes data in a JSON-encoded format. This 653 byte data is therefore received by the Arduino and stored in its buffer memory, just like the fingerprint module itself does store prints data being checked in the buffer memory on the Arduino stored in its buffer memory, just like the fingerprint module itself does store prints data being checked in the buffer memory on the Arduino.

From this stage, the Arduino quickly checks which of the ports is available counting up from storage port 0 of 10, then stores in the first available port using the same storage mechanism provided by the makers of the fingerprint module, all these are done within 6 seconds. The system was configured to check the online database for a new print, so that the extra six seconds delay would be avoided, but this process takes a lot of the Arduino memory, so it was technically better to check only at the point of placing any finger for access.

One of the major challenges faced during the development process was memory management, as an Arduino has a very low memory level, and the code written takes a good percentage of this memory as well. With the help of the IDE used, the total memory usage of the code was calculated; therefore, continuous optimization of the code for minimal memory usage was possible and done.

IV. SYSTEM TESTING, RESULTS AND DISCUSSION

During testing, different scenarios were tried which shows different performance. An instance of testing phase was shown in Figure 6.

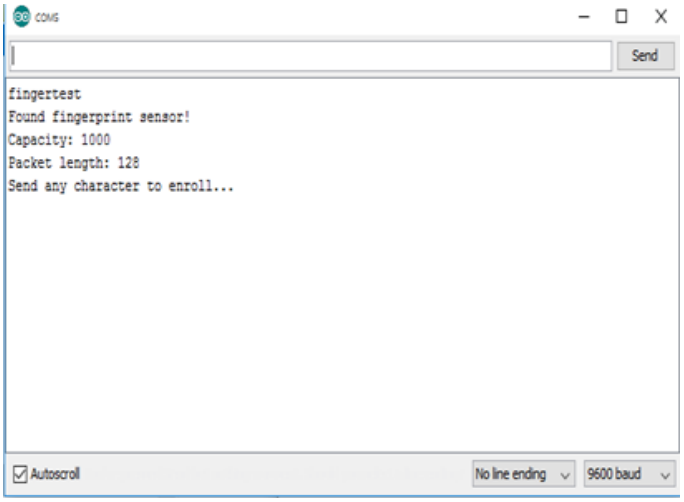

Figure 6: Fingerprint Sensor captured data.

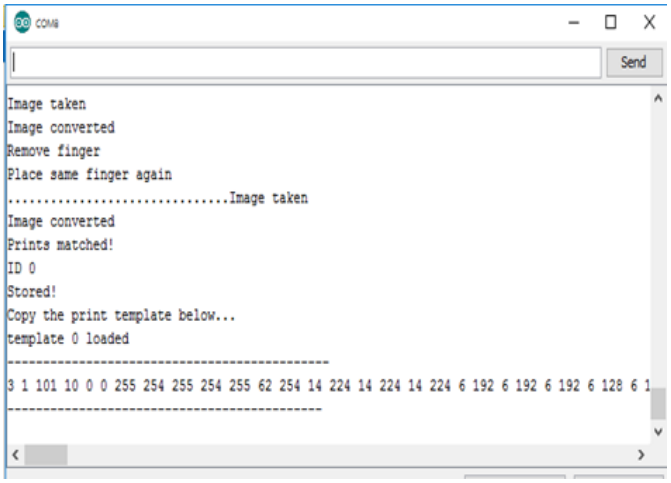

Figure 7: Fingerprint captured data template.

The sensor was able to read and match a wet finger but failed when tested with an oily or muddy finger. Under normal or dry condition, the sensor detects saved prints without anomalies. This leads to 95% success rate of the developed system during testing. Figure 7 shows a captured data template. It was observed that oily and muddy fingers were difficult to read by the fingerprint scanner. This system using fingerprint technology was able to find most matches of the prints stored on the webserver during testing, but when the connection to the internet is bad, it was unable to find match on the webserver.

V. CONCLUSION

In this work, a model of an IoT-based fingerprint-controlled door system that uses multi access authentication method was presented. The system architecture resent how different components exchange data through IOT. The Circuit Diagram for the system was designed to specify various modules inter-connectivity. The design implementation presented allows customer fingerprint templates captured while booking for rooms physically or remotely and fingerprint template captured at the entrance of each room to be stored on the web server. Finally prototype system unlocks the door only when both captured fingerprints templates matches.

Authors intend to integrate iOS touch ID with the fingerprint sensor of the door lock to share a common fingerprint database so that users can enrol their fingerprints directly from their phones. Furthermore, the door system availability can be extended to android platforms, a speaking voice alarm to indicate the unauthorized person accessing the Door and the proposed system can be made to communicate with modems or mobile phones to alert the authentic user an the hotel management during his tenancy period on every false attempt on the door.

REFERENCES

Aii, N. C. (2002). Broadband CSV, XML Alarm data Standards. NZ, Auckland.

Akhtar, L. P. (2017): IoT based Autonomous Office Alarm and Access Control System, Master's Thesis, Technical University of Denmark; www2.imm. dtu.dk/pubdb/ views /edoc_download. php/7034/pdf/imm7034.pdf

Aru, O. and G. Ihekwe. (2013). Facial Verification Technology for Use in ATM Transactions. American Journal of Engineering Research (AJER), 2(5): 188-193

Burak, S; K. Tolga; and K. Huseyin. (2015). Real Time Smart Door System for Home Security. International Journal of Scientific Research in Information Systems and Engineering (IJSRISE), 1(2):1-6.

Djupsjo, K. and M. Almosawi. (2018). IoT Security Applied on a Smart Door Lock Application. Unpublished M.Sc Thesis, KTH,tockholm;www. divaportal.org/ smash /get/diva2:1216681/FULLTEXT01.pdf

Falohun, A. S; E.O. Omidiora; O.A. Fakolujo; O, A. Afolabi; A.O. Oke and F.A. Ajala. (2012). Development of a biometrically-controlled door system (using iris), with power backup. American Journal of Scientific and Industrial Research, 3 (4): 203-207.

Fredrick, R. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. International Journal of Programmable Device Circuits and Systems, 6(6): 64-69.

Hitachi, R. (2004). Door-access-control System Based on Finger-vein Authentication. Hitachi Review 53(2):79-82.

Jain, A.K; A. Flynn and A. A. Ross. (2007). Handbook of Biometrics, Springer, Netherlands.

Mohd, S.S. (2005). Prototype Security Door Access System. An M.sc thesis, Faculty of Computer Science and Information Technology, University Pura Malaysia. http://psasir.upm.edu.my/id/eprint/5861/1/FSKTM_2005_10(1-24).pdf

Nehete, P. R; J. P. Chaudhari; S. R. Pachpande and K. P. Rane. (2016). Literature Survey on Door Lock Security Systems International Journal of Computer Applications 153(2):13-18.

Pankanti, S; S. Prabhakar and A. K. Jain. (2002) On the Individuality of Fingerprints, IEEE Trans. Pattern Analysis and Machine Intelligence, 24(8): 1010-1025.

Shoewu, O; O.M. Olaniyi and A. Lawson (2011). Embedded Computer-Based Lecture Attendance Management System. African Journal of Computing and ICT. 4(3): 27-36

Wildes, R. (1997). Automated iris recognition: An Emerging Biometric Technology. Proceeding of the IEEE 85(9): 1348-1363.

Woodward, O. and M. Higgins (2003). Biometrics/ Authentication Technology on the web at biometrics. pbworks.com/w/page/14811351/Authentication/1/212019 technologies.

Zorzi, M; A. Gluhak; S. Lange and A. Bass. (2010). From today's intranet of things to a future internet of things: a wireless- and mobility-related view. IEEE Wireless Communications. 17(6):44-51.

Appendix I: C Code Snippet for the System Prototype Implementation

```
#include <SoftwareSerial.h>
#include <FPM.h>
#define BUFF_SZ 512
#define to_use 0
// Download a template, delete it, print it, and upload it to a different flash location
// pin #6 is IN from sensor (GREEN wire)
// pin #7 is OUT from arduino  (WHITE/YELLOW wire)
SoftwareSerial mySerial(7,6);

int getFingerprintEnroll(int id);

FPM finger;

void setup()
{
 Serial.begin(9600);
  Serial.println("fingertest");
 mySerial.begin(57600);

 if (finger.begin(&mySerial)) {
   Serial.println("Found fingerprint sensor!");
 Serial.print("Capacity: "); Serial.println(finger.capacity);
 Serial.print("Packet length: "); Serial.println(finger.packetLen);
 } else {
 Serial.println("Did not find fingerprint sensor :(");
 while (1);
 }
 Serial.println("Send any character to enroll...");

while (Serial.available() == 0);
getFingerprintEnroll(to_use);
 delay(3000);
Serial.println("Copy the print template below...");
 getTemplate(to_use);  // download template at #4 (if it exists)       to the buffer; first enroll a finger at that
location
 }

void loop()
{
}
```