iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34309

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Smart Lock for Hostel Student based on IOT

Vishakha S. More[1], Pranali V. Sapkale[2], Dhanshri J. Jadhav[3], Pragati S. Patil[4], Ms. Tejaswini Pawar[5]
[1, 2, 3, 4] *Student,* [5] *Professor, Department of Information Technology, Karmaveer Adv. Baburao Thakare College of Engineering, Nashik, India.*

Abstract: ***Conceptual Security has systematically been a major worry to the overall public either within the family units or the geographic point condition. There are many different methodologies have been used to deal with these problems. The venture is planned in such a way that it has designed a savy lockup framework by using the Internet of Things. Since the long time ago, the usage of standard keyed locks have been basic. Anyway there is always a higher risk of keys being stolen, going in inappropriate hands or lost. Later, several people started using biometric locks replacing ancient keyed locks to enhance the security of their luggage. In replication to the traditional lock, an upto-date biometric lock do not need key and instead uses a biometric sensor. Our project is based on node MCU which is mostly adaptable operating device that insures physical safety by using the biometric sensor element that is accessible in a smartphone with the help of application. This determined technique during the study uses the IOT technology which therefore uses the smartphone application communication technology for standard device (smart lock for Hostel) to lock or unlock a lock through application. Above all, this study proposes the sensible Smart Lock for Hostel primarily based on security for the protection issue caused by the physical key utilized in hostel lockers, lockers at the houses, lockers at the offices, lockers at the hotels, etc.***

Keywords: Internet of Things, Arduino, Smart lock, smart locker, Android, GPS module.

I. INTRODUCTION

Now a day's individuals face a lot of issues concerning security. Security is the most essential issue all over the world, the major purpose of this paper is to frame and implement a locker with higher security system based Fingerprint and Image process technology which might be organized in bank, hotels, secured offices, hostels and houses. With this system a complete authentic person will unlock the lock. We've designed a locker security system based on finger print and Image processing technology supporting door lockup system which might compare, evidence, and identify the user and open the door in real time for locker secure access[1,2].

The Internet of Things (IoT) holds the promise to bring huge benefits for users, industry, and society by combining the capabilities of collecting large amount of data over long periods of time with substantial processing capabilities and low-latency communication. However, the convergence of these technologies raises significant security and privacy concerns. To mitigate these risks, access control plays a key role for providing controlled information sharing—a necessary condition to build privacy into IoT solutions— and integrity guarantees—a crucial pre-requisite for the correct functioning of an entire IoT system

Ancient approaches to access control are not sufficient for IoT due to somel sources of complexity, consisting the heterogeneity and huge number of connected devices (e.g, different types of sensors distributed in many locations), resource constraints (on processing, storage and communication), interaction patterns (from stable and long-lived to casual and short-lived), and augmented context awareness (such as time, location, and mode of operation of a system) [13]. The deployment of secure and privacy-aware IoT solutions with negative consequences on their adoption by users only because of a lack of belief.

II. METHODOLOGY

A. User Registration & Permission Configuration

The smart lock manufacturer provides users with a mobile application and a unique authorization code along with the smart lock. After installing the application, the owner pairs the application with the smart lock using the provided unique authorization code. Then, the owner can generate short term and long term digital keys for various types of users (family members, visiting friends, etc.) by accessing the access management system in manufacturer's private cloud. The access to the private cloud is controlled with the usage of One Time Password (OTP) generated by the application on the owner's mobile device [1, 3].

B. Locking and Unlocking Process

The smart lock is controlled through a smart lock application provided by the manufacturer and installed on the user mobile device. A user can LOCK or UNLOCK the lock through the smart lock's mobile application. As shown in Figure 1, when a user enters the

©IJRASET: All Rights are Reserved

Bluetooth range of the smart lock, his mobile phone is authenticated and paired with the smart lock through the Bluetooth protocol. Once connected, the smart lock receives the key status of the specific user from the remote access management system via the user's mobile device and uses the received key status to determine whether access should be granted. The local database of the smart lock also stores the key status. In case if the remote access management system might have been unable to reach, the smart lock system makes sure that the availability and maintain access by deciding on the basis of the entries in its local database [2, 4].

III. IMPLEMENTATION

A. *Software Implementation*

We have developed one android app named 'Smart Lock' which will be used to operate the locker. Firstly user have to register with app so that he will get access to locker. And once user have registered successfully then after just simple login process he will be able to access all the functionality of app.

Following are the basic operations performed by this app:

1) Through this app user can lock and unlock the locker at any time by just clicking on 'Lock' and 'Unlock' commands.

2) In the case where user got notified with a text of security alert , that means if someone tries to unlock the locker in absence of user the IR sensor will detect the human and a text message of security alert or we have termed it 'Suspecious opening of locker found' will be sent to user.

3) After receiving the notification on mobile the user can open to app and click on the command 'Capture Image' to see who is there around locker. This is because of the spy camera which is fitted on surface of locker.

4) Sometimes we need any document or material from our locker but we are out of home at that emergency cases we used to share a password with someone else in traditional locker system, there was risk of that third person may misuse the password till we come home and reset it. So we have overcame this issue, in such emergencies we can ask that third person to install this app on his phone and user need to share a security code with him , after that the person will be able to unlock locker using app command.

5) With respect to above case, we have added one security option where user can check logs of locking and unlocking of locker by that third person. So user will get to know if that person has misused app or not.

B. *Hardware Implementation*

The locker model have fingerprint scanner fitted on front surface which will be used for purpose of unlocking of locker.Firstly new user that is student will be registered with that scanner so that he will get access locker through fingerprint scanner.

The next module of hardware is Bluetooth module , it is used for data transmission purpose between Arduino nano and Android App . There is one IR sensor present on the surface of locker which will detect the human near locker and it will send a text of security alert to user.

The core of hardware is arduino nano which connects aal these modules together with locker system. There is on spy camera used for image capturing purpose. If any specious activity of unlocking ocker found and a user received security text and that if that activity is unknown of user then user can capture image just by giving a capture command through android app installed on his phone. This will be helpful for claiming the complaint.

Rather than using non rechargeable batteries we have used small android phone which is not only replacement for battery but also will be used for gps tracking feature in future. So here we can charge battery through USB port of phone. Because of phone the lock module got optimised and weight is also got reduced. This lock made for locker is multipurpose lock we can also fit it in traveling bags also. Here user don't need to remember password at all because he will have two options for unlocking one will be fingerprint scanner and another will be through an App.

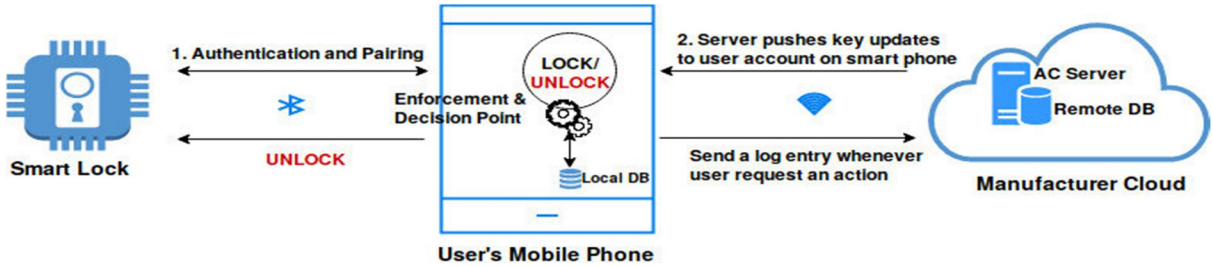


Fig 1: Architectural Design of the Smart Lock System

©IJRASET: All Rights are Reserved

IV. ARDUINO NANO

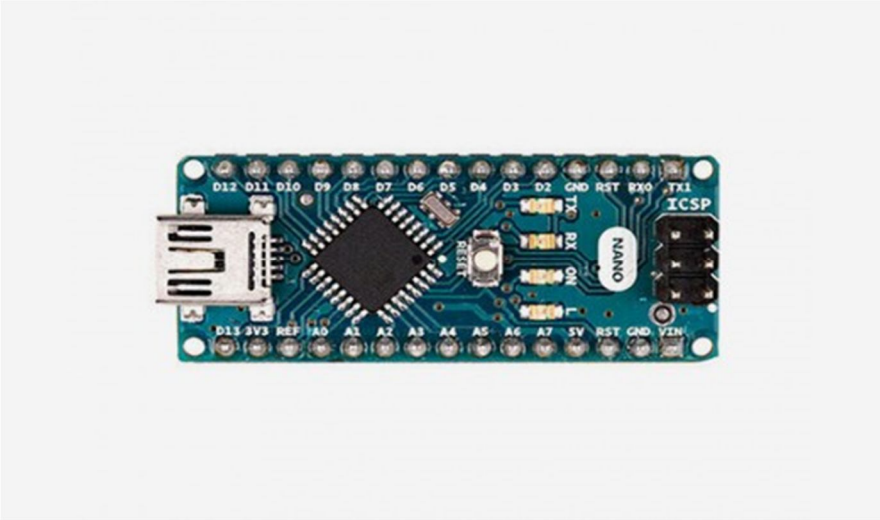


Fig 2: Arduino Nano Module

The Arduino Nano is a very compact, complete, and breadboard-friendly board supported by the ATmega328. It does not has only a DC power supply, and operates with a Mini-B USB cable rather than a standard one. The power can be given to the Arduino Nano board via Mini-B USB connections. The first one is 6-20V unregulated external power source (pin 30), or another one is 5V regulated external power source (pin 27). The selection of the power source is automated to the highest voltage supply. The ATmega328 has 32 KB of storage, (also the boot loader uses the 2 KB). The ATmega328 has storage of 2 KB of SRAM and 1 KB of EEPROM. Each one of the 14 digital pins on the Nano can be used as an input or output, using functions like pinMode(), digitalWrite(), and digitalRead(). They works at 5 volts. In addition, some pins have specialized functions [5].

V. FINGERPRINT SENSOR

This is the optical biometric fingerprint sensor module which has TTL UART interface for connecting directly to a microcontroller UART. The fingerprint data can be saved by the user in the module to configure it in 1:1 or 1: N mode for identifying the person. The module can directly interact with any of the 3.3V or 5V microcontrollers, but a suitable level of serial adapter is suggested for interacting with the serial port of a computer. The processing of fingerprint includes two parts. One is fingerprint enrolment and another is fingerprint matching. While enrolment of user, he needs to input the fingerprint two times. Then the system will process these two fingerprint images and it will generate a template of the fingerprint which will rely on processed results and saved template. At the time of comparing fingerprints, the user will input the finger through optical sensor, after which the system will create a template of the fingerprint for comparing it with the library of the fingerprint templates [3].

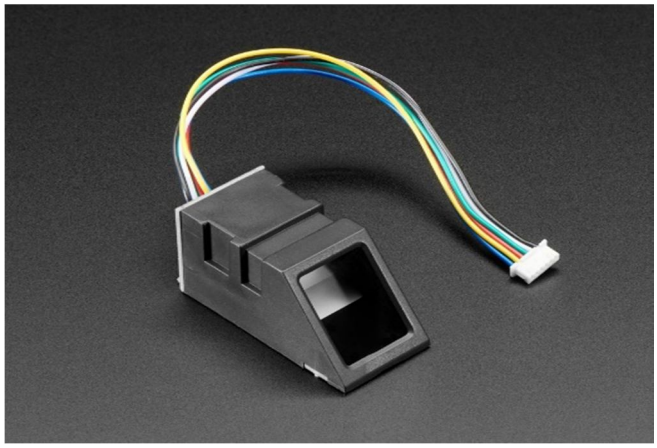


Fig 3: Fingerprint Sensor Module

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

VI. FINGERPRINT SCANNING MECHANISM

Fingerprint technology is one of the most evolving biometric modality which allow us to identify the identity of individuals. Fingerprints are very unique and even identical twins can also be identified with the help of biometrics. It is a highly accurate and reliable identity verification method. Fingerprint matching compares the very unique features like the characteristics of minutia patterns or ridges that are found within the fingerprint pattern. This fingerprint sensing process generally combines of capturing the fingerprint image, extracting the differentiating features of the fingerprint, and then saving a digital template of the fingerprint or comparing the current image with the saved fingerprint templates [4].

Fig 4: Fingerprint Scanning Mechanism

VII. RELATED WORK

A. *Fingerprint Lock System*

As Fingerprints are the formation of ridges through the mixture of genetics and environmental factors, fingerprint lock gives access to only that person whose fingerprint is already stored within the memory. Therefore PIN or password hacking is impossible. Also, one do not need to the combination of PINs and passwords to keep in mind. Even in the situations like power failure or battery drainage, stored fingerprints can be retained [1].

1) *Smart Bag with Theft Prevention and Real Time Tracking:* Data taken from ultrasonic and IR sensor. To measure distance between bag and human by sending sound waves and collects the reflected waves when it tracks an obstacle ultrasonic sensor is employed. Mislay or loosing of bag is additionally avoidable using proximity detection method. Beyond this it's feature of tracing and tracking the bag using GPS and GSM and locate the accurate position of the bag. Fingerprint locking system is used in this project. For charging of mobile phones and laptops Recharging port is also provided in this project as an in built power bank [1].
2) *Luggage Tracking System using IOT:* GPS (Global Positioning System) module, alarm and an Arduino board are connected with the other components of the system. The location of the bag can be traced by using synchronized map. An alarm notifies the user about passing of the bag beyond the particular range from its owner. Alarm would help the user to trace the bag but if bag crosses the map area fed into the server, user cannot trace the bag [2].
3) *Design of Bag Monitoring Security System Based On Internet of Things:* Most common belongings that lost, stolen, drop, or not monitored because of our activity are wallet, suitcase, and bag. If those item taken, impossible will retrieve back. Bag watching security system based on Internet of Things may be a resolution for acknowledge of bag condition. Is our bag open or shut, whether or not it way or close to North American nation, or wherever is that the precise position of our bag on the globe. This method is exploitation Arduino as microcontroller, Bluetooth module as distance indicator, sim 800L module to send information to cloud server and create a decision to grant notification of opened bag, GPS module to acknowledge bag location, and wire app to show notification of each request to the system. Output of this analysis may be a system that capable to show notification for user with eight second delay notification [3].
4) *Automated Luggage Carrying System:* In this paper various methods like Radio Frequency Identification (RFID), smart cards, synchronous rotation of motors and ultrasonic sensors are used. The locomotion function used here can make wheels to move forward and backward, if three wheels rotate right the other three wheels rotate left and vice versa. An embedded integrated circuit included in a smart card that is either a microcontroller or a memory chip. The bag can detect the obstacles due to the presence of ultrasonic sensors. It does not have a mobile application. The cost of RFID for long distance is more and if the short range Radio Frequency Identification (RFID) is used then finding the bag will be tedious work [4].
5) *Improved Baggage Tracking, Security and Customer Service with RFID in Airline Industry:* In this paper the frequency Identification (RFID) is employed for identification of the luggage and therefore the Customers. The frequency Identification (RFID) is attached as tags on luggage and within the tickets. The frequency Identification (RFID) readers keep track of the bags of the purchasers. It has three level of testing, they are unit testing for giving an error-free system, system testing is used to check whether the work is compatible and is harmonious to every other and acceptance testing is that the final testing process and then is suggested for the users. It can be implemented only in the airports. It can be implemented for all destinations in the airlines network [5].

©IJRASET: All Rights are Reserved

VIII. CONCLUSION

In this paper, a smart lock with advanced security feature is designed to work on the Internet of Things. We analyzed a realistic smart lock solution and identified the main requirements that access control systems for IoT should satisfy. Driven from this analysis and the current state-of-the-art IoT platforms, we presented a solution that outsources the specification and administration of access control policies to a trusted third party, while leveraging the access control mechanism available in the IoT platform for policy evaluation and enforcement. We investigated the practical feasibility of the proposed approach and discussed how the identified requirements are satisfied.

The designed smart lock senses the impact of an invalid visitor and alerts the user giving notification on the users mobile. It can be used in every household, in office or in hotel's to minimize the human efforts and can save a lot of time. It nullifies risk of keys getting lost or stolen. As the system is online, a person can lock/unlock from anywhere around the world at his own comfort. The registered user can check the logs for locking/unlocking at at any time to avoid any theft activities.

REFERENCES

[1] Álvaro Alonso, Federico Fernández, Lourdes Marco, and Joaquín Salvachúa. 2017. IAACaaS: IoT Application-Scoped Access Control as a Service. Future Internet 9, 4 (2017), 64.

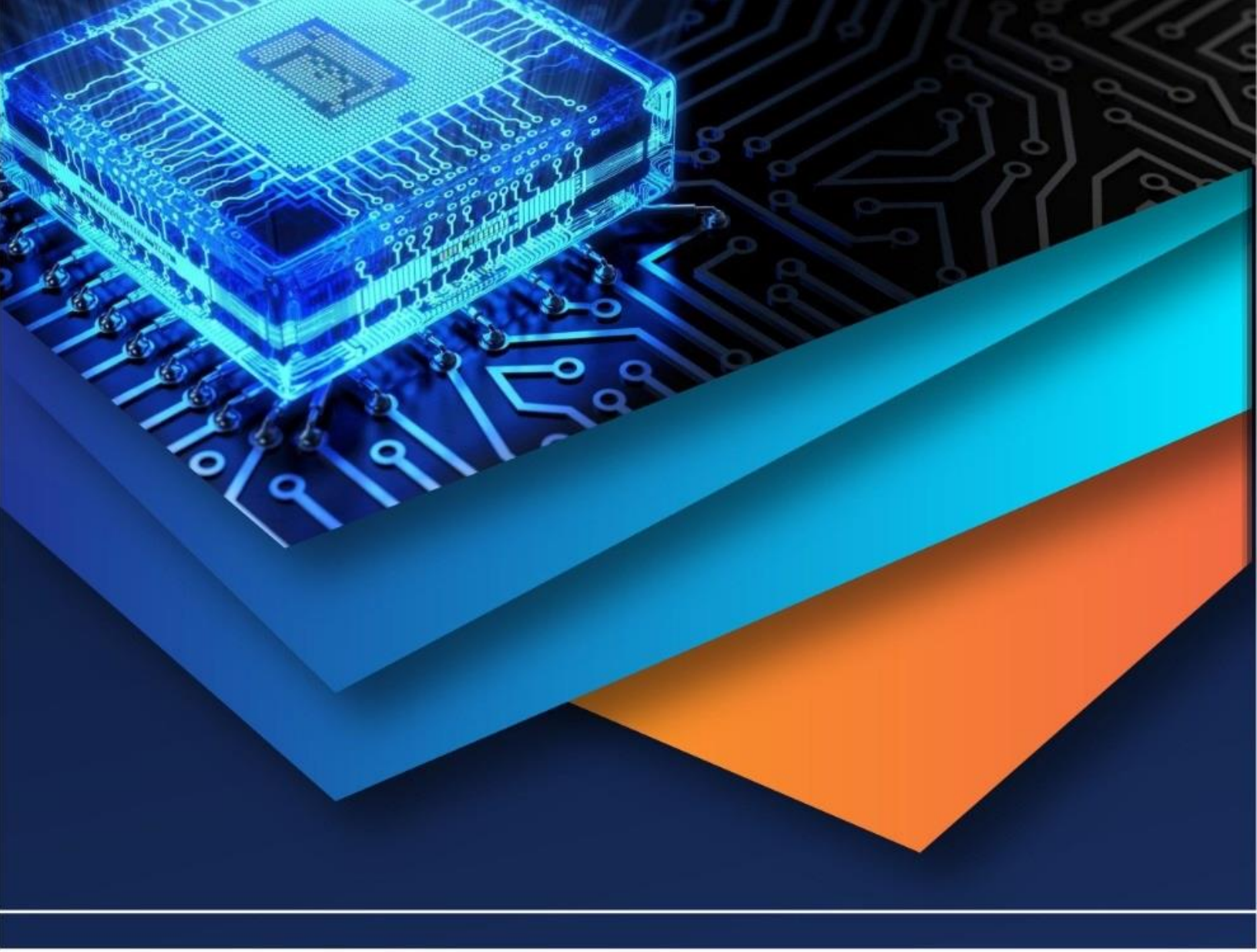
[2] A. Armando, S. Ranise, R. Traverso, and K. S. Wrona. 2016. SMT-based Enforcement and Analysis of NATO Content-based Protection and Release Policies. In Proc. of the ABAC@CODASPY 2016. 35–46.

[3] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. Access Control Model for AWS Internet of Things. In Int. Conf. on Network and System Security. Springer, 721–736.

[4] Charles C Byers. 2017. Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for FOG-enabled IoT networks. IEEE Communications Magazine 55, 8 (2017), 14–20.

[5] David F Ferraiolo, Ravi Sandhu, Serban Gavrila, D Richard Kuhn, and Ramaswamy Chandramouli. 2001. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 4, 3 (2001), 224–274.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)