School

of

Electronics And Communication Engineering

Mini Project

on

A BANK LOCKER SECURITY SYSTEM

By:

1. **Divya Hegde** USN:01FE20BEC091
2. **Kavya Hegde** USN:01FE20BEC093
3. **Soumya H J** USN:01FE20BEC097
4. **Vaishnavi Shetti** USN:01FE20BEC101

Semester: V, 2022-2023

Under the Guidance of

Dr.Sujata S Kotabagi

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2022-2023

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **"Bank locker security system"** is a bonafide work carried out by the student team of **"Divya Hegde (USN: 01FE20BEC091) , Kavya Hegde (USN: 01FE20BEC093), Soumya H J (USN: 01FE20BEC097) and Vaishnavi U Shetti (USN: 01FE20BEC101)"**. The project has been approved as it satisfies the requirements with respect to the mini project work prescribed by the university curriculum for BE (V Semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2022-2023.

Dr. Sujata S Kotabagi	Dr. Nalini C Iyer	Dr. Basavaraj S A
Guide	Head of School	Registrar

REGISTRAR
KLE Technological University
HUBBALLI-580 031.

External Viva:

Name of Examiners **Signature with date**

1. Basawaraj
2. Dr. D A Toose
23/12/22

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2022-2023

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **"Bank locker security system"** is a bonafide work carried out by the student team of **"Divya Hegde (USN: 01FE20BEC091) , Kavya Hegde (USN: 01FE20BEC093), Soumya H J (USN: 01FE20BEC097) and Vaishnavi U Shetti (USN: 01FE20BEC101)"**. The project has been approved as it satisfies the requirements with respect to the mini project work prescribed by the university curriculum for BE (V Semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2022-2023.

Dr. Sujata S Kotabagi	Dr. Nalini C Iyer	Dr. Basavaraj S A
Guide	Head of School	Registrar

REGISTRAR
KLE Technological University
HUBBALLI-580 031.

External Viva:

Name of Examiners	Signature with date
1.	

ACKNOWLEDGMENT

Without the assistance and cooperation of a lot of individuals this project's completion would not have been feasible. But we'd like to say this instead: we owe our mentors and managers a huge debt of gratitude for their unending support. We would like to thank them for their patience, kindness, and understanding throughout the project. we useful advice and concepts. Additionally, we appreciate our college for giving us all the project's necessary resources Overall, we want to express our gratitude to all those involved in this project and provided us with advice to improve the project. In the end, would like to thank our parents and friends for being there for us and helping us in every way possible.

-The project team

ABSTRACT

The focus of this project will be on creating a reliable identifying and controlling system for completely autonomous bank locker rooms. Our security system can recognise unauthorised entrances in the locker room area, which are frequently used in robberies. Banks won't be able to identify the burglar in the event of a heist since there isn't enough proof using the present human-operated security system. Thanks to the development of multiple sensors, systems today include a significant number of preventive and remedial procedures. In order to offer a workable security solution for extremely important and private data and items, we presented an Automated Safety Vault with Double Layered Defense Mechanism. A password-controlled electronic lock was part of the solution.

Contents

List of Figures

Chapter 1

Introduction

Today's fast-paced environment requires high levels of security. People are now more conscious about their possessions, including priceless papers, cash, jewellery, and other items. The bank is the best location to store all of these items. Every person engages in banking transactions on a daily basis. Thus, the banking industry need rigorous security. The bank locker system now uses a two-key system, one of which is kept by the customer and the other by the relevant bank employee. If one of the keys is missing, the situation gets worse because both keys are required to open the locker. There are numerous ways created to keep bank lockers secure thanks to technological innovation. Electronic security systems are becoming more advanced, but they are still all manual.

1.1 Motivation

Given the state of technology today, nothing should be insurmountable. Our suggestion offers a system that is highly secure, legal, and simple to use for both bank customers who have lockers there and the branch manager who is in charge of all activities related to the safety lockers. Our job involves user fingerprint verification as well as authentic login information for authorised users. The main goal of the suggested method is to provide the outcomes of group decision-making based on the information offered by several sensors.

1.2 Objectives

For a wide range of commercial and security applications, an effective, low-power, and low-cost embedded access control system is crucial for Smart Bank security and remote monitoring based on motion detection.

- This idea suggests using the Internet of Things (IoT) to send images to the user's Gmail account and allow safe access to only approved people via SMS.
- When someone tries to enter the bank locker, the Raspberry Pi records the attempt and processes the image before sending it as a picture message to the user's Gmail account.
- The user can then give the Raspberry Pi permission to open or remain closed using his or her Gmail account. As a result, for a highly secure locker

1.3 Literature survey

In order to understand the existing works in the context of the proposed idea, the following papers are discussed.

[1]Locker Security System Using RFID and GSM Technology by Aruna.D. Mane and Sirkaz Mohd Arif May,2013 The Atmel AT89C52 microcontroller verifies the ID number that the RFID reader reads from the passive tag before sending it. If the ID number is legitimate, the microcontroller will use GSM to send an SMS request to the cellphone of the verified person. To provide access, the microcontroller confirms the password.

Advantages: GSM and passive RFID are more secure than other technologies.

Disadvantages: For network unavailability, lockers cannot be opened.

[2] "Enhancing ATM Security Using Fingerprint And GSM Technology" by Ashish M. Jaiswal and Mahip Bartere April,2014 After inserting his or her card, the client entering the ATM must place their finger on the fingerprint sensor module in order to receive an automatic 4-digit code that is sent via GSM modem attached to the microcontroller to the authorised customer's mobile device each time.

Advantages: The user will benefit from strong authentication.

Disadvantages: It takes time in the beginning due to the various verifications.

[3] Web-based online embedded door access control and home security system based on face recognition developed by Mrutyunjaya Sahani and Chiranjiv Nanda. Written in 2015. Face detection and recognition algorithms are employed, together with a wireless interface, to recognise visitors and send an email and/or alert message to the house owner's mobile phone or other communication device regarding the present state of the home environment.

Advantages: It increases security.

Disadvantage: Face detection requires a more complicated algorithm.

[4] S. Tanwar, S. Tyagi, and M.S. A cutting-edge security alert system for smart homes based on the Internet of Things. written in 2017. when no one is present at home to notice an intruder or any unexpected event. A tiny pyroelectric infrared (PIR) module and raspberry pi are used in this low-cost home security system to save processing time for email alerts.

Advantages: Cheaper and more secure.

Disadvantage: The security alert warning is only provided via email.

[5] "Design and implementation of an SMS-based home security system," by Biplav Choudhury, Tameem S. Coudhur, Aniket Pramanik, Wasim Arif, and J. Mehendi, was published in August 2015. The project includes two Android applications for user interaction with the hardware, an 8 bit ATmega16 microcontroller, and a GSM SIM900A module. When the panic button is pressed, the emergency contact receives the emergency message and the sender's GPS location. No matter where it is deployed, the device, which costs less than 1300INR, may be used as long as there is mobile network connectivity.

Advantages: Secure and affordable

Disadvantages: Mobile network connectivity is necessary

[6] Biometric and GSM Security for Lockers, Sagar S. Palsodkar and Prof. S.B. Patil, December 2014. This article suggests a biometric (finger or face) and GSM-based locker system for security. When a user's user name and password match, their face is identified, and a code is transmitted to their mobile device through GSM and requested on a computer, if this code matches, the locker will unlock.

Advantages: The GSM and biometric measurement are both well-liked.
Disadvantages :Large data space required.

[7] Design and implementation of an SMS-based home security system, Biplav Choudhury, Tameem S. Coudhury, Aniket Pramanik, and Wasim, August 2015. The project includes two Android applications for user interaction with the hardware, an 8 bit ATmega16 microcontroller, and a GSM SIM900A module. When the panic button is pressed, the emergency contact receives the emergency message and the sender's GPS location.

Advantages: Lower cost; no need for network connectivity.
Disadvantages: Less secure.

[8] P. Sugapriya and K. Amsavalli stated in their article "Smart Banking Security System Using Pattern Analyzer" that pattern flow is initially gathered as datasets and kept on a bank agent server. The device has a camera to record the user's pattern of movement, which is then transferred for processing where elements of the logic were matched and the user was identified.

Advantages: Greater security due to the usage of three levels of banking security.
Disadvatages:Time-consuming due to the need for enormous datasets.

[9] Sanal Malhotra, "Banking Locker System With Odor Identification Security Question Using RFID GSM Technology," This paper describes a mechanism for identifying odours in banking locker security. Everyone in this world has a unique odour, which aids the system in differentiating and identifying individuals. This method of identifying smells makes use of an electronic nose. The technology behind the electronic nose is called e-sensing.

Benefits: More secure.
Cost-effectiveness is a disadvantages.

[10] The bank locker security system based on RFID, GSM, Conveyer, Microcontroller, and Heat sensor was described by Prof. R. Srinivasan, T. Mettilda, D. Surendran, K. Gobinath, and P. Satishkuma in their paper, "ADVANCED LOCKER SECURITY SYSTEM." Locker users must first swipe their RFID tags, which include details about them such as their locker number and other information. Once the tag has been verified as being legitimate, the bank manager will deliver the appropriate locker via a conveyer configuration. In addition, if someone tries to access the locker with a tool or machine, a heat sensor will catch the theft. Temperature will rise if a burglar uses an instrument, which will be detected and cause an alarm to go off.

Provides extra security features, which is an advantage.
Disadvantages: Time consuming.

1.4 Problem statement

"Develop a high security locker system for bank sector using IOT(internet of things) to provide secure access only to authorized person via biometric , password and also sending image to the user G-mail account"

Chapter 2

System design

System design, as seen in figure 2.1, includes a full description of the functions that the system should carry out as well as various approaches for fulfilling these functions. Finally, the best design is selected from the several design possibilities.

2.1 Functional Block Diagram

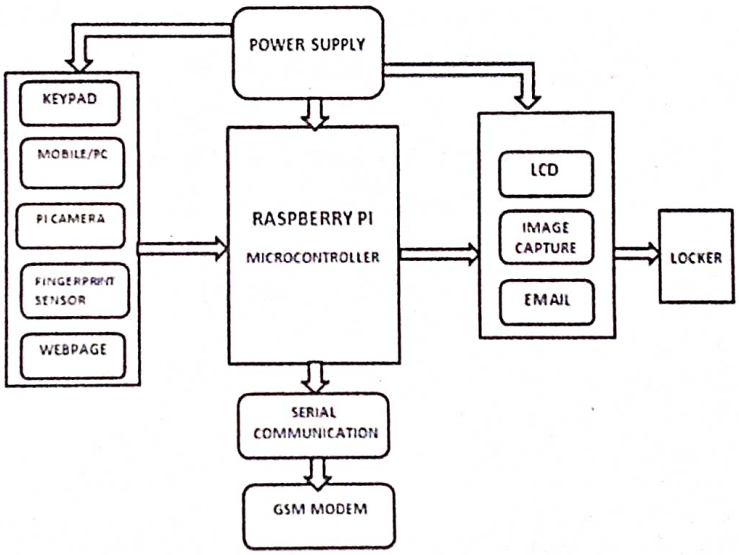

Figure 2.1: Functional Block Diagram [8]

2.2 Design alternatives

1. BANK LOCKER SECURITY SYSTEM USING QR CODE SCANNING:

   - Consider two QR codes: one that is permitted and the other that is unlawful.

- If the allowed code is displayed, the bank locker will open, the green led will turn on, and it will also turn on when the bank locker is closed.
- The bank locker will remain closed (with the red led on) and the buzzer will sound if an unlawful QR code is displayed.

2. BANK LOCKER SECURITY SYSTEM USING BIOMETRIC :

- Recognisation of face: First, we must store the allowed person's face pattern. The face is then scanned when opening and closing the locker and compared to the face of the authorized user. If the faces match, the locker will open; otherwise, it will remain closed and the buzzer will sound.
- Palm : First, we need to store the authorized person's palm pattern. The palm is then scanned and matched with the authorized person's palm during locker opening and closing. If the palms match, the locker will open; otherwise, it will remain closed and the buzzer will sound.
- Utilizing Retina : First, we must keep the authorized person's retina. when the door is opened and closed

3. BANK LOCKER SECURITY SYSTEM USING PASSWORD AND OTP :

- In this approach, the password is entered via the keyboard; if the password is correct, an OTP is sent to the registered phone number, which must then be entered before the locker can unlock.
- If the password is correct but the OTP is input incorrectly, an alarm message will be sent to a registered phone number.
- If the password is wrong, the locker won't open and the buzzer will go off.
- If a user enters a wrong password three times, they will not be able to do so again for 24 hours.

4. SECURITY SYSTEM FOR BANK LOCKERS USING KNOCK-OUT GAS

- This inbuilt device ensures bank security by emitting knock-out gas. It is only open during bank closing times. The sensor next to the locker notices an attempt to rob the bank and alerts the microcontroller when it does so. The relay circuit activates when the signal from the microcontroller is given to it, turning on the gas-releasing apparatus and enabling the release of the knock-out gas for a predetermined period of time. A knock-out gas is released, which renders the robber unconscious. A higher-ranking Bank official's cellphone that uses GSM technology receives the signal from the microcontroller as well. Bank security staff members may easily apprehend the perpetrators with the help of the police. This recommended bank security solution is an entirely automated.

2.3 Final design

We select one of the optimal solutions based on its working and ease of the implementation.

We settled on the final design for a bank locker system that uses a password, fingerprint, image capture identification, and an OTP for further protection. This is the greatest option because it has two-step verification and a highly secure mechanism, making it more secure than any other option. It offers security even when the user is not present physically by verifying that a recorded image is legitimate and transmitting it to the user's email address.

Chapter 3

Implementation details

This chapter contains all the details that have been considered while designing the Bank locker security system.

3.1 Specifications and final system architecture

- For implementation Raspberrypi3 and GSM SIM900A has been used.
- The following simulation tools have been installed.
  - Raspberry pi imager
  - VNC viewer
  - IDLE tool
  - Proteus
  - PuTTY

3.2 Algorithm

- Step1: Start
- Step2: Set the static password
- Step3: Consider Keypad as an input and LCD as an output
- Step4: Enter the password
- Step5: If password is correct then lock1 is open.
- Step6: Place the finger on the touch sensor.
- Step7: If fingerprint is correct locker2 will open.
- Step8: Else it will send captured image to registered email id.
- Step9: Then it will send OTP.
- Step10: If the entered OTP is correct then locker2 will open
- Step11: Stop

Chapter 4

Flow chart

4.1 Flow chart of the implementation of the project.

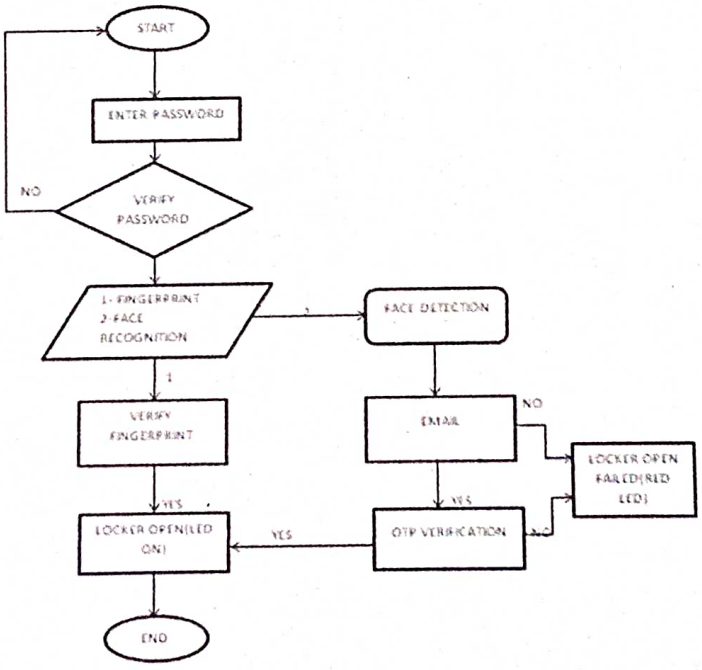

Figure 4.1: Flow chart [8]

Chapter 5

Results and discussions

This part discusses about results obtained by simulation done in Proteus platform.

5.1 Result Analysis

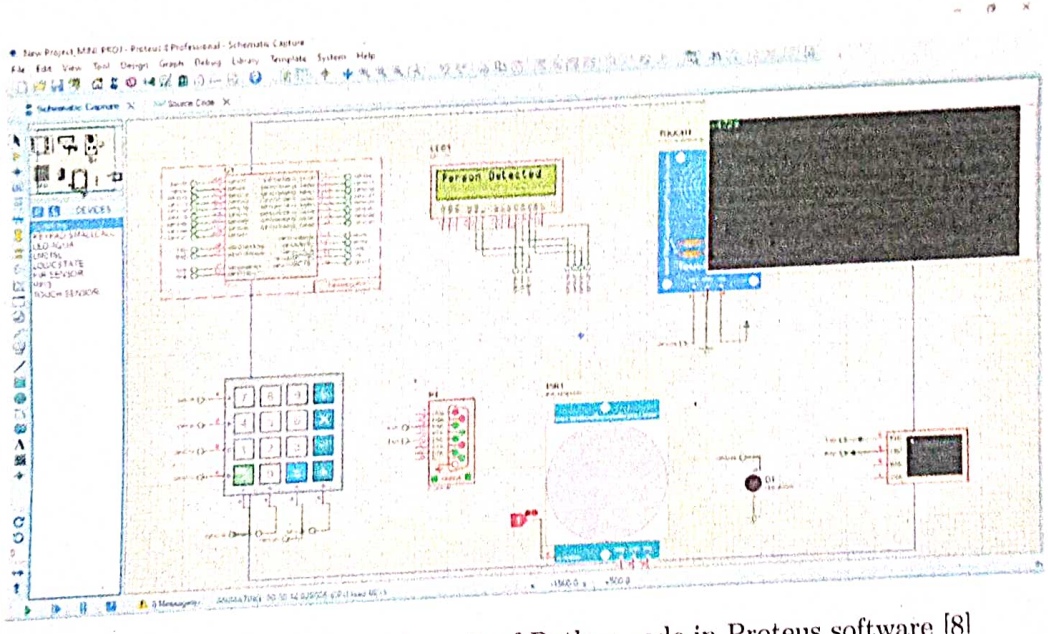

Figure 5.1: Simulation and result of Python code in Proteus software [8]

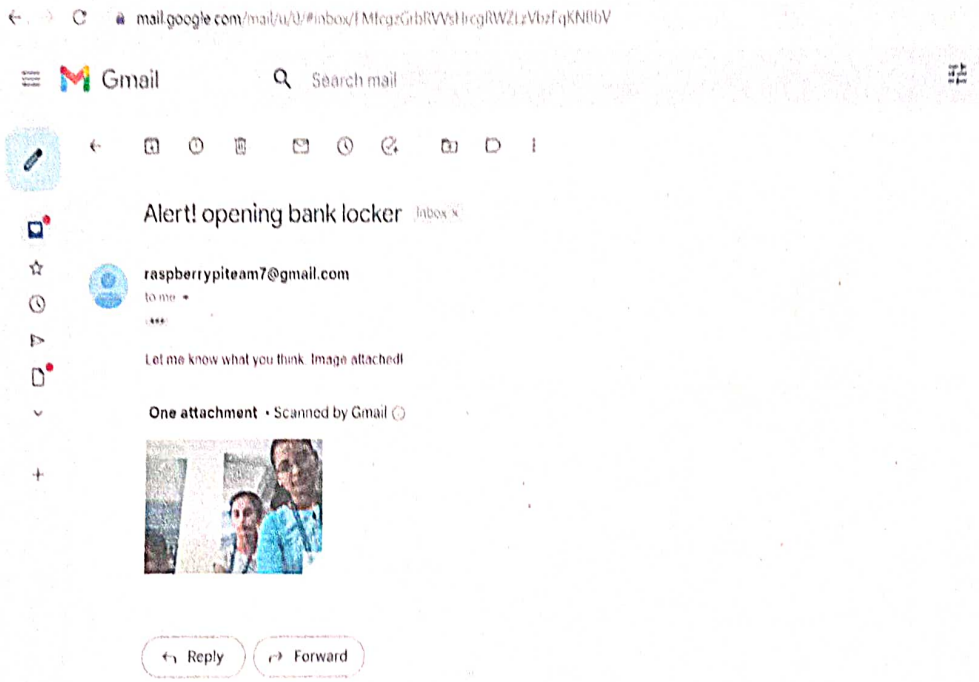

Figure 5.2: Sending captured image to registered email id through GSM modem using AT command [8]

Chapter 6

Hardware implementation

6.1 Hardware setup

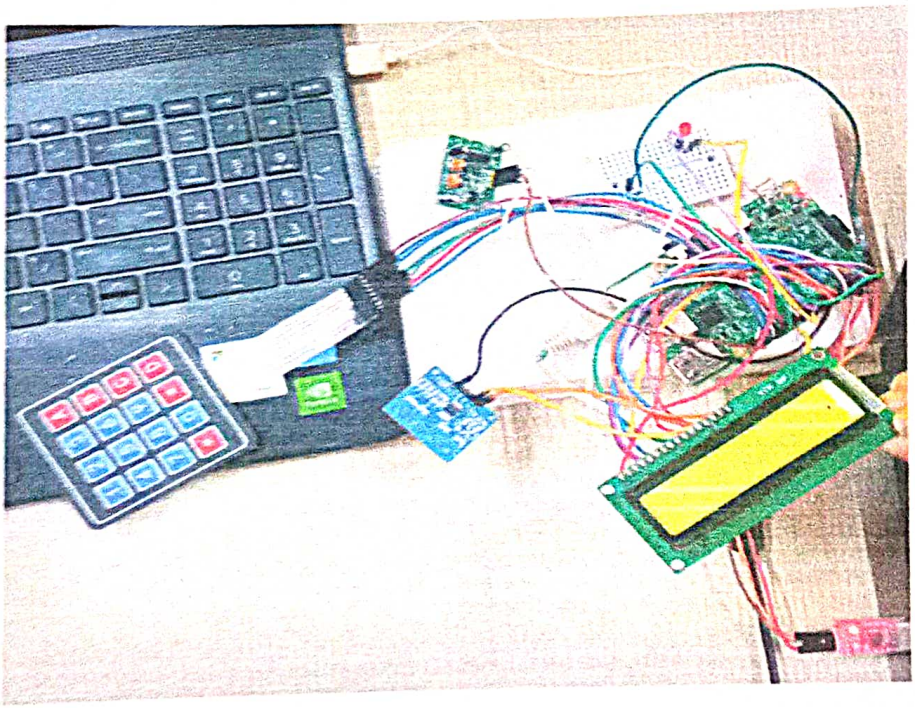

Figure 6.1: Hardware implementation[8]

6.2 Conclusion

It is clear from this project that we have created a highly secure bank locker system. To open the locker, we employed a password, biometric, face recognition system, and OTP, providing dual layer security. More security is provided even when the person is not present physically.

Bank_locker_security_system

ORIGINALITY REPORT

13%	10%	6%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijert.org Internet Source	3%
2	J. Chinna Babu, K. Naveen Kumar Raju. "Chapter 39 Safety Locker System with Image Identification by Using IOT", Springer Science and Business Media LLC, 2022 Publication	2%
3	www.coursehero.com Internet Source	2%
4	wineyard.in Internet Source	2%
5	1library.net Internet Source	1%
6	S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, M. S. Obaidat. "An advanced Internet of Thing based Security Alert System for Smart Home", 2017 International Conference on Computer, Information and Telecommunication Systems (CITS), 2017 Publication	1%

7	www.cse.ust.hk Internet Source	1 %
8	www.e-ijaet.org Internet Source	1 %
9	conferenceworld.in Internet Source	<1 %
10	www.researchgate.net Internet Source	<1 %
11	www.seekdl.org Internet Source	<1 %
12	www.engpaper.com Internet Source	<1 %
13	www.rtsoft.ru Internet Source	<1 %
14	Biplav Choudhury, Tameem S. Choudhury, Aniket Pramanik, Wasim Arif, J. Mehedi. "Design and implementation of an SMS based home security system", 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015 Publication	<1 %
15	www.semanticscholar.org Internet Source	<1 %