

GLOBAL JOURNAL

OF COMPUTER SCIENCE AND TECHNOLOGY: E

Network, Web & Security

Preserved Level of Privacy

Trust-Based Security Technique

Highlights

Anti-Phishing Protection System

BER Performance Analysis of OFDM

Discovering Thoughts, Inventing Future

VOLUME 20 ISSUE 3 VERSION 1.0



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY

VOLUME 20 ISSUE 3 (VER. 1.0)

OPEN ASSOCIATION OF RESEARCH SOCIETY

© Global Journal of Computer Science and Technology. 2020.

All rights reserved.

This is a special issue published in version 1.0 of "Global Journal of Computer Science and Technology" By Global Journals Inc.

All articles are open access articles distributed under "Global Journal of Computer Science and Technology"

Reading License, which permits restricted use. Entire contents are copyright by of "Global Journal of Computer Science and Technology" unless otherwise noted on specific articles.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission.

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website <http://globaljournals.us/terms-and-condition/menu-id-1463/>

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

(A Delaware USA Incorporation with "Good Standing"; Reg. Number: 0423089)

Sponsors: Open Association of Research Society

Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America

USA Toll Free: +001-888-839-7392

USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please
email us at local@globaljournals.org

eContacts

Press Inquiries: press@globaljournals.org
Investor Inquiries: investors@globaljournals.org
Technical Support: technology@globaljournals.org
Media & Releases: media@globaljournals.org

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

EDITORIAL BOARD

GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY

Dr. Corina Sas

School of Computing and Communication
Lancaster University Lancaster, UK

Dr. Sotiris Kotsiantis

Ph.D. in Computer Science, Department of Mathematics,
University of Patras, Greece

Dr. Diego Gonzalez-Aguilera

Ph.D. in Photogrammetry and Computer Vision Head of
the Cartographic and Land Engineering Department
University of Salamanca Spain

Dr. Yuanyang Zhang

Ph.D. of Computer Science, B.S. of Electrical and
Computer Engineering, University of California, Santa
Barbara, United States

Dr. Osman Balci, Professor

Department of Computer Science Virginia Tech, Virginia
University Ph.D. and M.S. Syracuse University, Syracuse,
New York M.S. and B.S. Bogazici University, Istanbul,
Turkey

Dr. Kwan Min Lee

Ph. D., Communication, MA, Telecommunication,
Nanyang Technological University, Singapore

Dr. Khalid Nazim Abdul Sattar

Ph.D, B.E., M.Tech, MBA, Majmaah University,
Saudi Arabia

Dr. Jianyuan Min

Ph.D. in Computer Science, M.S. in Computer Science, B.S.
in Computer Science, Texas A&M University, United States

Dr. Kassim Mwitondi

M.Sc., PGCLT, Ph.D. Senior Lecturer Applied Statistics/
Data Mining, Sheffield Hallam University, UK

Dr. Kurt Maly

Ph.D. in Computer Networks, New York University,
Department of Computer Science Old Dominion
University, Norfolk, Virginia

Dr. Zhengyu Yang

Ph.D. in Computer Engineering, M.Sc. in
Telecommunications, B.Sc. in Communication Engineering,
Northeastern University, Boston, United States

Dr. Don. S

Ph.D in Computer, Information and Communication
Engineering, M.Tech in Computer Cognition Technology,
B.Sc in Computer Science, Konkuk University, South
Korea

Dr. Ramadan Elaiess

Ph.D in Computer and Information Science, University of
Benghazi, Libya

Dr. Omar Ahmed Abed Alzubi

Ph.D in Computer and Network Security, Al-Balqa Applied
University, Jordan

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Dr. Rajesh Kumar Rolan

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - Microsoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

CONTENTS OF THE ISSUE

- i. Copyright Notice
 - ii. Editorial Board Members
 - iii. Chief Author and Dean
 - iv. Contents of the Issue
-
1. Smart Air Conditioner using Internet of Things. ***1-38***
 2. Trust-Based Security Technique to Curb Cooperative Blackhole Attacks in Mobile Ad Hoc Networks using OTB-DSR Protocol in NS-3. ***39-54***
 3. BER Performance Analysis of OFDM, W-OFDM and F-OFDM for 5G Wireless Communications. ***55-63***
 4. A Secure Big data Framework Based on Access Restriction and Preserved Level of Privacy. ***65-75***
 5. No Fish; Total Anti-Phishing Protection System. ***77-83***
 6. QoS Evaluation of SIP Signalled VoIP Network Routed using MANET Routing Protocols. ***85-90***
-
- v. Fellows
 - vi. Auxiliary Memberships
 - vii. Preferred Author Guidelines
 - viii. Index



Smart Air Conditioner using Internet of Things

By Khaloud Bati AL-Sa'idi & Dr. Vladimir Dyo

University of Bedfordshire

Abstract- The local remote control is the traditional mechanism in which the end user controls the air conditioner. In the absence of this mechanism, the user loses the control. This thesis aimed to design and implement a smart air conditioner using Internet of Things (IoT) technology. Recent Literatures were reviewed to select the most optimal platform to design and implement the project. The design of the project was then developed based on the selected platform. The project was then implemented and tested successfully. In order to validate the project, a questionnaire was carried out by potential users who tested the product on their SANYO air conditioner. All potential users were able to control their air conditioner remotely over the internet from anywhere. The smart air conditioner has absolutely no inference against real remote control. The product is cost effective, energy efficient and achieves the required automation functionality.

GJCST-E Classification: C.2.6



SMARTAIRCONDITIONERUSINGINTERNETOFTHINGS

Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

Smart Air Conditioner using Internet of Things

Khaloud Bati AL-Sa'idi ^α & Dr. Vladimir Dyo ^σ

Abstract- The local remote control is the traditional mechanism in which the end user controls the air conditioner. In the absence of this mechanism, the user loses the control. This thesis aimed to design and implement a smart air conditioner using Internet of Things (IoT) technology. Recent literatures were reviewed to select the most optimal platform to design and implement the project. The design of the project was then developed based on the selected platform. The project was then implemented and tested successfully. In order to validate the project, a questionnaire was carried out by potential users who tested the product on their SANYO air conditioner. All potential users were able to control their air conditioner remotely over the internet from anywhere. The smart air conditioner has absolutely no inference against real remote control. The product is cost effective, energy efficient and achieves the required automation functionality.

I. INTRODUCTION

As it is known, the usual and traditional mechanism in which the end user controls the air conditioner is through local remote control. However, what if the local remote control is lost, broken, out of batteries or no longer available due to whatever faulty?

On the other hand, what if the air conditioner is forgotten on due to human nature and no one is available to turn it off?

How about controlling the temperature degree of your air conditioner while you are actually away?

How about having a smart air conditioner that would be able to turn off by itself when people are not present and save energy?

Reaching this point, Automation feature seems the best logical solution to handle and control the air conditioner remotely.

Nowadays, Internet of Things (IoT); an emerging technology has risen in the digital realm. The original idea of Internet of Things was proposed at the end of 1990's. IoT is much more related to the wireless sensors networks, mobile communications networks and Internet. IoT can be defined as a network that connects every existing physical object in the world to a unique address in order to provide quick and smart services. In contrast to traditional Internet which interconnects intelligent physical objects only, IoT interconnects both intelligent and non intelligent physical objects due to the availability of object sensing layer (Ma, 2011).

Hence, with Internet of Things, you may control everything using internet service. More specifically, through Internet of Things technology, you will be able to

Author ^α σ: MSc. (Computer Networking), University of Bedfordshire, 2016. e-mail: khaloud.al-saidi@study.beds.ac.uk

remotely control your air conditioner which will be connected to the internet from anywhere.

Internet of Things technology uses cost effective, powerful and small size device that is considered to be a small size single board computer called Raspberry Pi. Raspberry Pi was developed by Raspberry Pi Foundation. There are four different types of Raspberry Pi such as: Original Raspberry Pi, Raspberry Pi, Raspberry Pi 2 and Raspberry Pi 3. The four different types come with both Model A and Model B flavors. Different platforms can be used as an Operating System for the Raspberry Pi such as: RISC OS, Arch Linux, Pidora, Raspbian and Microsoft Windows 10 IoT core (Harrington, 2015).

The aim of this project is to design and implement a smart air conditioner using Internet of Things technology using Raspberry Pi 3 Model B device.

The aim of this project is accomplished through fulfilling pre-defined objectives. Starting with reviewing related home automation system literatures. Moving to selecting the most suitable platform (Raspbian: the most popular platform used with Raspberry Pi or Windows 10 IoT core: the new platform developed by Microsoft) to design and implement the smart air conditioner. Testing, validating and exploring the gained features of the product are the final step towards accomplishing the project aim.

The features of the designed smart air conditioner were decided through testing the implemented product by potential users. The smart air conditioner has absolutely no inference against real remote control. The product is cost effective, energy efficient and achieves automation functionality indeed.

Each implemented project must involve intellectual challenges. Apparently, there are implemented air conditioner projects using Internet of Things raspberry Pi with different web and mobile enabled applications. However, in this project the web application is developed using PHP web language and MySQL database engine which are not used by any of the developed projects.

Internet of Things means any physical object is connected to the internet. In this system, a smart air conditioner which can be controlled remotely through a web application is to be implemented. However, in order to control the air conditioner remotely, it must be connected to the internet in the first place. Obviously, the air conditioner does not have any internet connection port. Hence, it will be connected to the raspberry pi 3 that has the required internet connection



port. The connection between the air conditioner and the raspberry pi 3 is through the Infra-Red (IR) transmitter which is a Lite Emitting Diode (LED) emitting Infra-Red lights (connected to the raspberry pi 3) and Infra-Red (IR) receiver. Then, the internet connection port in raspberry pi 3 will be connected to Wi-Fi hot spot in order to get internet service. On the other hand, any physical device such as: a desktop, a laptop, a PAD

and a smart phone which has a web browser in order to use the implemented web application is connected to the internet from anywhere to control the air conditioner remotely. Furthermore, the implemented air conditioner would be able to turn off by itself when people are not present.

The following figure illustrates the above mentioned project specifications.

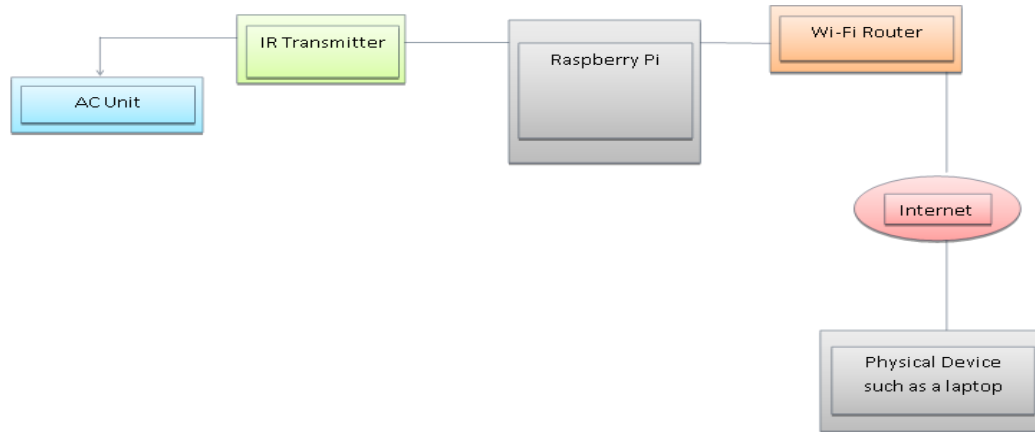


Figure 1: Smart Air Conditioner Using Internet of Things System Specifications

II. LITERATURE REVIEW

Home automation systems have been a successful revolution in the technology world. Extensive researches were conducted on home automation systems. Indeed, home automation systems still receive an inordinate attention from academic organizations and institutions.

Different technologies have been employed to build home automation systems, Al-Ali & Al-Rousan (2004) built a java-based home automation system where all home automated appliances were connected physically to an embedded board with integration to a Personal Computer acts as a web server which provided a remote access to the built system.

Java-based home automation system provides a secure solution due to the built-in security feature handed over by java technology. However, the system is not cost effective due to the need of high quality specifications of the Personal Computer as well as expensive installed wired environment. Furthermore, since the system depends mainly on wired communication, installation's intrusiveness is increased.

Sriskanthan et al. (2002) developed a Bluetooth based home automation system where each home physical appliance is connected to a local Bluetooth sub controller through wired connections. Each appliance communicates with the local Bluetooth sub controller connected to and then all local Bluetooth sub controllers communicate with a primary controller through wireless connection.

In contrast to Java-based home automation system, Bluetooth based home automation system

architecture reduces intrusiveness of wired installation due to the use of wireless technology. Nevertheless, some intrusiveness is still there due to the wired communication between home appliances and Bluetooth sub controllers. Moreover, this system connects one Bluetooth sub controller to many home physical appliances due to the cost of Bluetooth technology where it is appropriate to have a dedicated Bluetooth sub controller for each appliance. Never forget to mention that the use of one Bluetooth sub controller shared between many home appliances actually causes access delay.

Zhu et al. (2010) proposed a Voice Control System for Zig Bee-based Home Automation system. Automatic speech recognition module is used to translate voice commands and send them to the actuator of the designed system via ZigBee network. Each automated home appliance is connected to a dedicated ZigBee module in order to operate and control it remotely.

Similar to Java-based home automation system, developing a Voice Control System for ZigBee based Home Automation system is not cost effective due to the expense of ZigBee module; hence the system is becoming uneconomical as the number of physical home appliances to be automated is enlarged. Furthermore, the speech recognition system must have a module which unfortunately causes errors due to the noise.

When reviewing academic researches on home automation systems, it is apparently that, the developed systems with different existing technologies such as Bluetooth, Java and ZigBee are facing some

imperfections and limitations such as the cost, access delay, wired installation intrusiveness and power consumption.

In this project, I selected different and innovative but existing technology which is Internet of Things (IoT). The reason behind using this technology in this project can be justified from my following findings on IoT technology.

Internet of Things is considered to be the revolutionary technology in the future of the internet (Gubbi et al., 2013).

Ma (2011) declared that the original idea of Internet of Things was proposed at the end of 1990's through MIT Auto-ID Labs. IoT is much more related to the wireless sensors networks, mobile communications networks and Internet. IoT can be defined as a network that connects every existing physical object in the world to a unique address in order to provide quick and smart Services (Ma, 2011).

IoT is a complicated technology and it consists of four layers; application service layer, information integration layer, data exchange layer and object sensing layer. Application service layer offers satisfied services to different users. Information integration layer integrates unclear information into usable knowledge, recombines and cleans unclear information attained from networks. Data transmission transparency is handled by data exchange layer. Sensing objects and obtaining data are handled by the forth layer which is object sensing layer. Never forget to mention that sensing feature is not supported by traditional Internet and accordingly it only interconnects intelligent physical objects. On the other hand, IoT interconnects both intelligent and non-intelligent physical objects due to the availability of object sensing layer (Ma, 2011). Table 1 summarizes limitations of different existing home automation technologies and IoT addressed solutions.

Table 1: IoT Addressed Solutions over Existing Technologies

Existing Technology	Short	IoT Addressed Solutions
Java-based home automation system	<ul style="list-style-type: none"> - High quality specifications of the Personal Computer acts as a Web Server - Expensive installed wired environment - High intrusiveness - High power consumption - Not cost effective 	<ul style="list-style-type: none"> - Cloud storage - Wireless connection - Intrusiveness free - Energy effective - Cost effective
Bluetooth based home automation system	<ul style="list-style-type: none"> - Low intrusiveness - Access delay 	<ul style="list-style-type: none"> - Wireless connection - Intrusiveness free
	<ul style="list-style-type: none"> - High power consumption - Not cost effective 	<ul style="list-style-type: none"> - Access delay free - Energy effective - Cost effective
ZigBee-based Home Automation system	<ul style="list-style-type: none"> - ZigBee module is expensive - Noise caused by Speech recognition module - High power consumption - Not cost effective 	<ul style="list-style-type: none"> - Noise free - Energy effective - Cost effective

Existing recent studies and conducted researches on controlling home appliances remotely mainly focuses on the use of IoT devices such as Raspberry Pi developed by Raspberry Pi Foundation. Raspberry Pi is cost effective, powerful and small size device that is considered to be a small size single board computer. Raspberry Pi may operate using different platforms; RISC OS, Arch Linux, Pidora, Raspbian and Microsoft Windows 10 IoT core (Harrington, 2015).

In this thesis, I will discuss two different platforms which are Raspbian, the most popular Operating System used for Raspberry Pi and Microsoft Windows 10 IoT core, the new raised Operating System developed by Microsoft.

Raspbian is an open source Linux based Operating System. It is a modified platform from Debian Operating System. Raspbian Operating System was developed exclusively for Raspberry Pi and hence it is



called Raspbian. Raspbian inherits almost all Debian features including above 35,000 free software packages. Beginners with Raspberry Pi are strongly recommended to start with Raspbian since it is designed for an easy use with different software packages (Harrington, 2015).

Windows 10 IoT core is an innovative version of Windows 10 and is targeting the small and embedded devices with or without display screens Raspberry Pi 2, Raspberry Pi3, Minnow Board MAX and Dragon Board 410c (Teixeira, 2015; Microsoft, 2016). Windows 10 IoT core intended to have a low barrier to access; hence making it easy to build professional devices. Windows 10 IoT core is compatible with different open source languages and works efficiently with Visual Studio platform as well (Teixeira, 2015).

Windows 10 IoT core brings all powerful features of Windows into your devices such as online storage, automatic Windows update through internet, user interface, security, Universal Windows Platform (UWP) APIs; the rich platform to easy control designed applications and cloud-based services (Microsoft, 2016; Anders, 2016).

Celebre et al. (2015) used Siri enabled mobile devices for remotely control home appliances, which are air conditioner unit, television, window blinds and lights using raspberry pi with Raspbian Operating System. In this system, the home appliances are connected to the raspberry pi through a relay and a motor driver. Both raspberry pi and Siri enabled mobile device are connected to the same local network (Celebre et al., 2015).

Rieger (2016) used raspberry pi, IR Diode, IR receiver and stepper motor to build a web interface to remotely control blind opener and air conditioner. The user accessed the web interface which transmits issued commands to a controller script. This system used raspberry pi with Raspbian Operating System.

Ivancreations.com (2016) built a mobile application and used Google voice recognition to remotely control Daikin air conditioner unit using raspberry pi and LED. In this system, the air conditioner unit is connected to the raspberry pi through Infra-Red transmitter LED. Both raspberry pi and the application based mobile are connected to the same local network through home Wi-Fi router (Ivancreations.com, 2016). The system is implemented using raspberry pi with Raspbian Operating System.

Vasanwala (2015) developed Home Automation using Raspberry Pi2 and Windows 10 IoT system. Lights, fans and wall sockets are connected to an Arduino – Internet of Things microcontroller device -. Each room must have its own Arduino connected to home appliances in that room, one Passive Infra-Red module, one temperature sensor that senses human presence and one LDR which detects light intensity. All

Arduino microcontrollers are then connected to the Raspberry Pi through I2C Bus. Basically, Arduino controls all home appliances and reads data from sensors and periodically sends those collected data to Raspberry Pi. Raspberry Pi sends data collected from Arduino microcontrollers to a wire frame application. You may control connected home appliances using wire frame application as well.

Low-cost Home Automation with Voice Control system is built by Gillett (2015). The system used Node.js server to control different existing hardware in a room such as: lights, door and LED Strip using Raspberry Pi. A web application is built based on voice control in order to control room's hardware remotely. When the user clicks on microphone button in the application, Raspberry Pi starts recording voice audio. The recorded audio is then sent to a natural language API called Wit.ai in order to analyze it and extracts the meanings. The extracted meanings are then sent back to Raspberry Pi in order to perform the action. The system is built using Raspberry Pi with Microsoft Windows 10 IoT core Operating System Platform.

Ganesan (2015) built WARAN – Home Automation system. WARAN is a modular system stands for Windows IoT, Azure, Raspberry Pi, Arduino, NRF24L01+ wireless solution. WARAN consists of one Hub acts as a control server and many modules such as: temperature sensor module and humidity sensor module which are connected to an Arduino. The basic functionality of the system is that the added modules read data and sends them to the Arduino through NRF24L01+. Arduino is then sends collected data from the sensors to the control server in Raspberry Pi through I2C Bus. Collected data from sensors such as: warnings and alerts in any module is also posted in a Windows phone application.

Through reviewing the above existing recent studies and conducted researches on controlling home appliances remotely, it is obvious that air conditioner appliance is successfully controlled remotely via Raspbian Platform using Linux Infrared Remote Control (LIRC). LIRC is an open source library that allows a user to record, decode and send Infra-Red signals of many standard remote controls (Bartelmus, 2016). On the other hand, there isn't any published system that controlled air conditioner remotely using Microsoft Windows 10 IoT core Platform. No one till now could implement any home appliance operates using Infra-Red signals using Windows 10 IoT core because it does not have any Infra-Red library. There were researches which attempted to automate home air conditioners using Win LIRC but they all failed. Win LIRC is Windows equivalent of LIRC which enables users receive and transmit Infra-Red signal of standard remote controls (Bailey et al., n.d.).

III. SYSTEM DESIGNN

Through reviewing different recent literatures demonstrated in CHAPTER 2, apparently there is a serious limitation with Windows 10 IoT core platform in reference to the lack of Infra-Red library. As a result, the most optimal platform to implement the smart air conditioner using Internet of Things is going to be Raspbian platform since it supports LIRC library. Before implementing the project, an overall design is built.

a) Web Application Wire Frame

The Wire Frame Design for the system is shown in Figure2. When the user who has a right access logs in the website, he will be able to see Control AC tab. The Control AC tab includes controlling AC power and the temperature of the air conditioner.

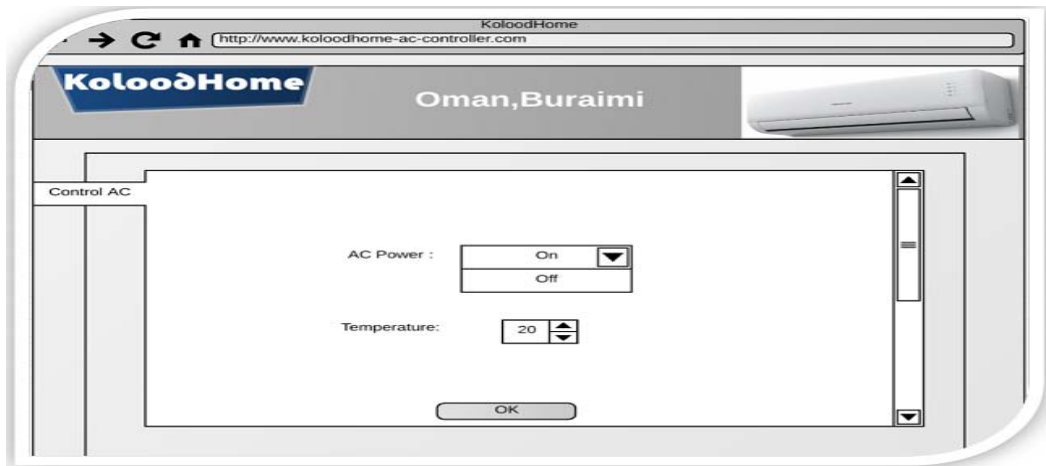


Figure 2: Web Application Wire Frame for Smart Air Conditioner Controller

b) Architecture Diagram

The system architecture includes the infrastructure and network design of the system. The web application will be designed using PHP web language and Raspbian will be the business logic for the design. The system architecture of the system is shown in Figure 3. My SQL server is used as web server to store data for web console and database server will

be hosted in LAMP in Raspberry Pi 3. VPN will be used between the LAMP and the Internet for security issue. PHP will be used as the front End and SQL database as the backend of the web application. The user can access the web application by writing the address in the web browser. On the other hand, the air conditioner is connected to the Wi-Fi at the same time.

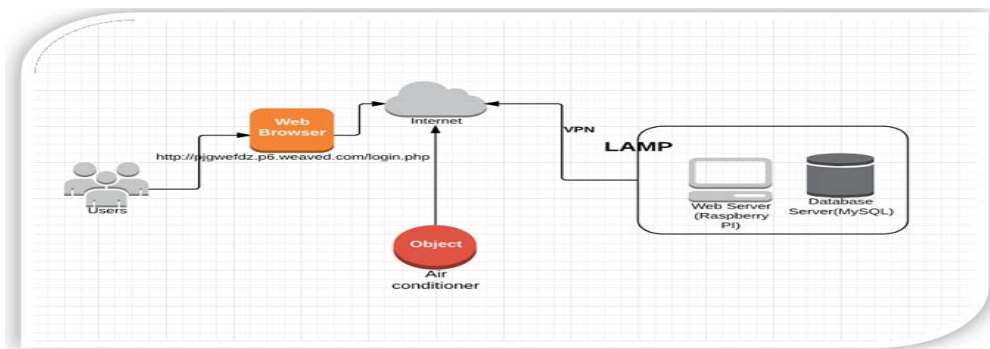


Figure 3: Architecture Diagram for Smart Air Conditioner Controller

c) Circuit Design

As mentioned earlier, air conditioner does not have an internet connection port. Hence, it will be connected to the raspberry pi 3 that has the required internet connection port. The connection between the air conditioner and the raspberry pi 3 is through the Infra-Red (IR) transmitter which is a Lite Emitting Diode (LED) emitting Infra-Red lights (connected to the raspberry pi 3) and IR receiver. Always remember that the circuit

needs resistors in order to control current flow and maintain the raspberry pi from damage. Figure 4 illustrates circuit design used in the project. IR LED is responsible of emitting infra-red signals and IR receiver is responsible of receiving infrared signals and modulating them. Basically this circuit design is going to be used to read SANYO air conditioner remote control and interpret its codes.

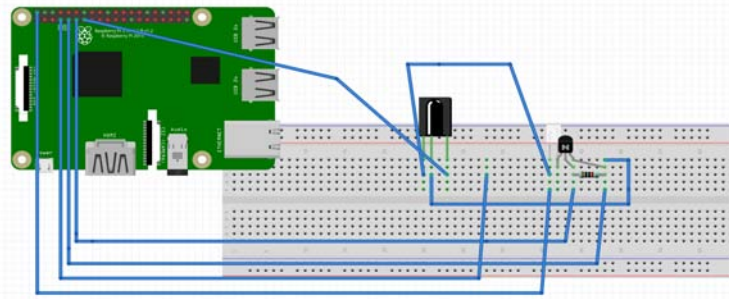


Figure 4: Smart Air Conditioner Circuit Design

IV. IMPLEMENTATION

a) *Hardware*

In order to implement the smart air conditioner, the following hardware is required:

- Raspberry Pi 3 Model B.



Figure 5: Raspberry Pi 3 Model B

- PIR (Passive Infra-Red) Motion Sensor



Figure 6: Passive Infra-Red Sensor

- SD Card (Minimum 8 GB).



Figure 7: SD Card

- SD Card Reader.
- IR Receiver.



Figure 8: IR Receiver

- IR Transmitter



Figure 9: IR Transmitter

- 10K ohm Resistor

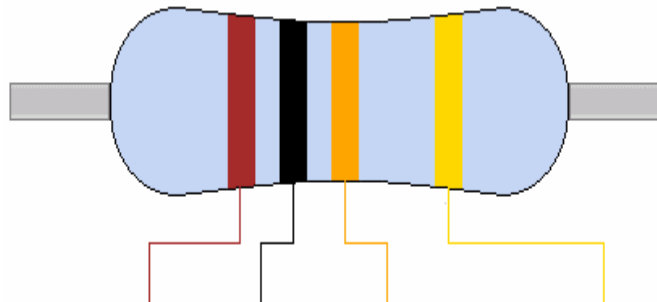


Figure 10: 10k ohm Resistor

- PN2222 Transistor

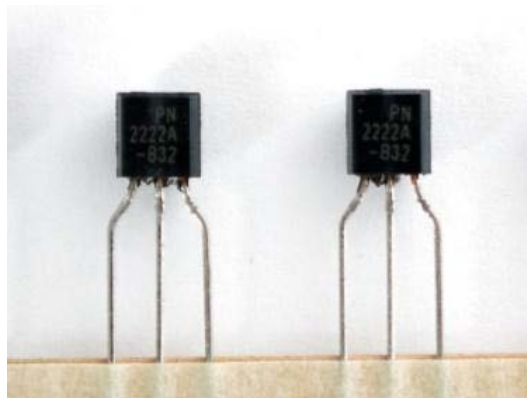


Figure 11: PN2222

- Wi-Fi Hot Spot.
- Monitor.
- USB Keyboard.
- USB Mouse.
- HDMI to VGA Cable.



Figure 12: HDMI to VGA Cable

- Solder less Bread Board

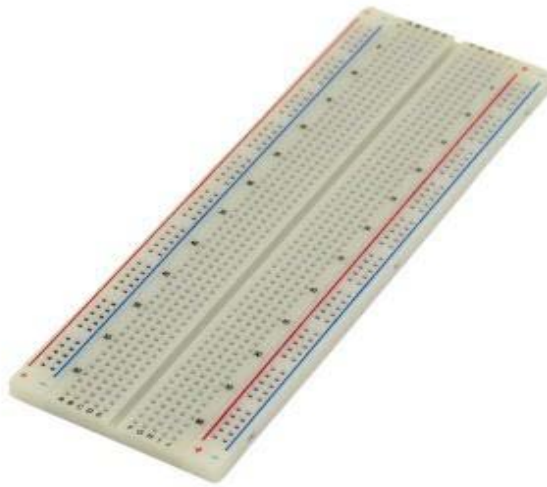


Figure 13: Solder less Bread Board

- Jumper Cables



Figure 14: Jumper Cables

b) Software

The following software packages are needed to implement the smart air conditioner:

- Raspbian Jessie Operating System (The full desktop image based on Debian Jessie).
- Wiring Pi.
- Linux Infrared Remote Control (LIRC).
- LAMP (Linux, Apache, MySQL, PHP) Web Development Platform.
- Python (The programming language that is pre-installed in Raspbian Jessie Operating System).
- Win32 Disk Imager.

c) Raspbian Jessie Operating System Setup

1. Download Raspbian Jessie Operating System image from the official site of Raspberry Pi: <https://www.raspberrypi.org/downloads/raspbian/>
2. Place 8 GB SD card into your SD card reader. In this project, I used the built in SD card reader in my laptop.

Figure: screenshot of Raspbian Jessie OS image mager

3. Mount the downloaded Raspbian Jessie Operating System image into your SD card using Win32 Disk Imager (if you are using Windows Operating System).

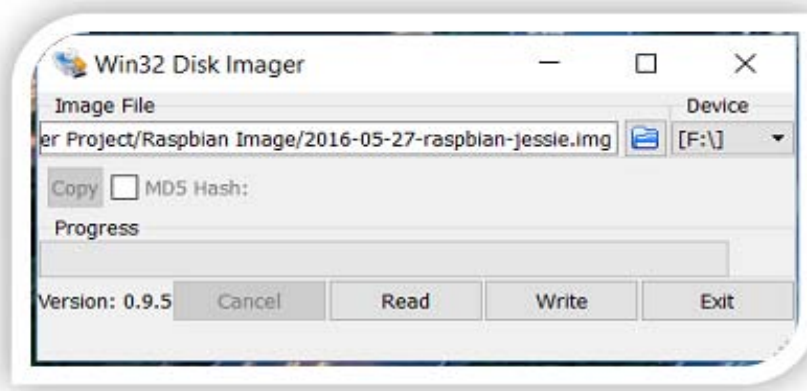


Figure 15: Win32 Disk

4. Eject your SD card from the SD card reader and mount your SD card into your Raspberry Pi 3.



Figure 16: SD CARD on Raspberry Pi 3 Model

5. Connect your Raspberry Pi 3 to your monitor using HDMI to VGA cable.
6. Connect your USB keyboard and mouse.
7. Connect the power cable of the Raspberry Pi 3.
8. Power on your Raspberry Pi 3.

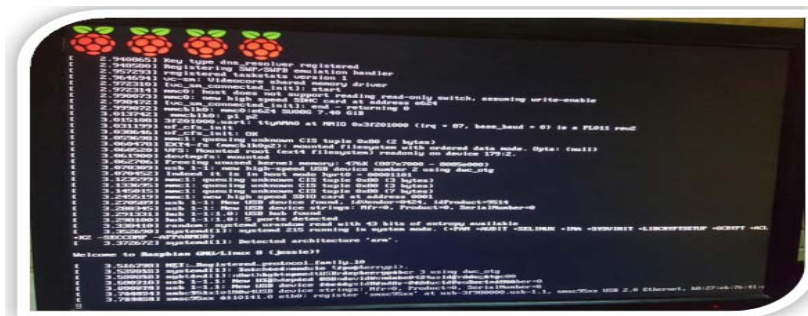


Figure 17: Screenshot of startup Raspbian Operating System



9. Test the raspberry Pi 3 by opening terminal window and type any command for example: hostname

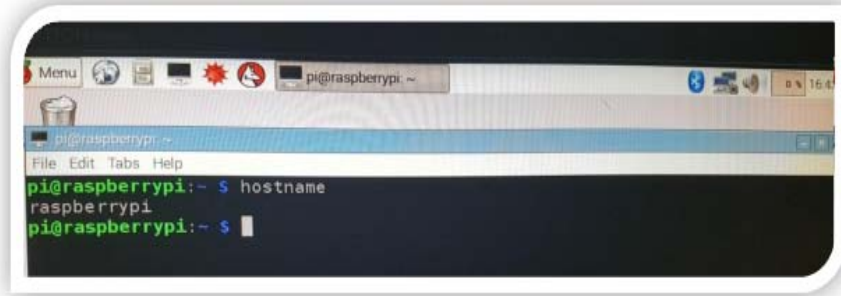


Figure 18: Screenshot of testing terminal window in Raspbian

d) *Wiring Pi Setup*

In order to control GPIO pins in your Raspberry pi 3 such as: read the pins, write the pins and control the pins from shell scripts, you have to setup Wiring Pi in your Raspberry Pi 3.

➤ Definition

Wiring Pi: is a GPIO access library used in Raspberry Pi and is written in C language (Wiring Pi, 2016).

The followings steps describe installation, setup and test of Wiring Pi in your Raspberry Pi 3:k

- 1) Connect your Raspberry Pi 3 to your wireless hot-spot using built in Wi-Fi dongle in your Raspberry Pi.
- 2) Open command terminal in your raspberry Pi 3.
- 3) Type the following command to setup GIT. Actually, GIT is maintained for Wiring Pi so that the user can easily track changes:

```
sudo apt-get install git-core
```

- 4) Type the following command to obtain Wiring Pi through GIT:

```
sudo git clone git://git.drogon.net/wiringPi5.
```

- 5) Type the following command to access WiringPi directory:

```
sudo cd wiringPi
```

- 6) Type the following command to install and build WiringPi library:

```
./build
```

- 7) Test Wiring Pi through typing the following command in terminal window:

```
gpio -v gpio readall
```

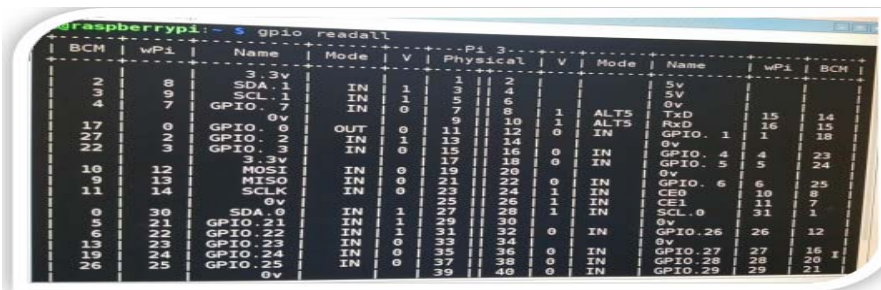


Figure 19: Screenshot of Testing Wiring Pi in terminal

e) *LIRC (Linux Infrared Remote Control) Installation and Configuration*

In order to be able to record your air conditioner remote control Infra-Red codes, you have to install and configure LIRC in your Raspberry Pi 3.

➤ Definition

LIRC: is an open source library that allows a user to record, decode and send Infra-Red signals of many – not all- remote controls (Bartelmus, 2016).

The followings steps describe installation and configuration LIRC in your Raspberry Pi 3:

1. Open command terminal in your raspberry Pi 3.
2. Type the following command to install LIRC library:

```
sudo apt-get install lirc
```

f) *LAMP (Linux, Apache, MySQL, PHP) Installation and Configuration*

In order to be able to record your air conditioner remote control Infra-Red codes, you have to install and configure LIRC in your Raspberry Pi 3.

➤ Definition

LAMP: is a web development platform used in Linux Operating System. It is the equivalent of WAMP (Windows, Apache, MySQL, and PHP) web development platform used in Windows Operating System.

The followings steps illustrate installation and configuration LAMP in your Raspberry Pi 3:

First: Apache Sever Setup

➤ Definition

Apache: is one of the most popular web server applications. It is installed in Raspberry Pi 3 to serve developed web pages by the user (raspberrypi.org, 2016).

Follow the following steps in order to install and configure Apache server:

1. Open command terminal in your raspberry Pi 3.
2. Type the following command to install Apache2 package:

```
sudo apt-get install apache2 -y3.
```

3. Open a web browser in your Raspberry Pi 3 and type: `http://localhost/` in order to test that Apache 2 server has been installed successfully.
4. Note that the default webpage `index.html` is stored in `/var/www/html` directory in your Raspberry Pi 3.

Second: PHP Setup:

➤ Definition

PHP: is one of the most popular web languages. It is a preprocessor that runs any received requests from a web page, process the requested page and sends it back to the web browser (raspberrypi.org, 2016).

Follow the following steps in order to install and configure PHP:

1. Open command terminal in your raspberry Pi 3.
2. Type the following command to install PHP 5 and Apache packages:

```
sudo apt-get install php5
libapache2-mod-php5 -y
```

3. Test PHP using steps listed below:

1. Create `test.php` file using the following command in terminal:

```
sudo leafpad test.php
```

2. Type the following PHP code inside `test.php` and save the file:

```
<?php echo "hello world"; ?>
```

3. Open a web browser in your Raspberry Pi 3 and type: `http://localhost/test.php`

Third: MySQL Setup

➤ Definition

MySQL: is one of the most popular database engines (raspberrypi.org, 2016).

Follow the following steps in order to install and configure MySQL:

1. Open command terminal in your raspberry Pi 3.
2. Type the following command to install MySQL server and PHP- MYSQL packages:

```
sudo apt-get install mysql-server
php5-mysql -y
```

3. While installing MySQL server, it will ask you to enter a root password in order to protect your server. Insert the password and remember it very well or you will lose your root access into MySQL server in your Raspberry Pi 3.

4. Type the following command to restart Apache server:

```
sudo service apache2 restart
```

g) *Implementation and Testing*

i. *LIRC Setup in Raspberry Pi 3:*

Prior implementing the project, you must setup LIRC in your Raspberry Pi 3. The following steps describe implementation of IR Receiver circuit:

1. Open command terminal in your raspberry Pi 3.
2. Type the following command to check GPIO output and input pins in Raspberry Pi 3 and select the appropriate for you:

```
gpio readall
```

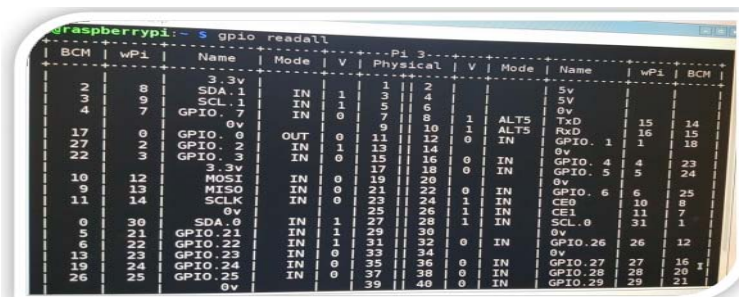


Figure 20: Screenshot of gpio readable command on Raspbian Operating

3. Type the following command to edit `modules` file:

```
sudo leafpad /etc/modules
```

4. Add the following two lines into `modules` file:

```
lirc_dev lirc_rpi
gpio_in_pin=17
gpio_out_pin=27
```

- ❖ *Note:* The added two lines specify that the GPIO input pin in Raspberry Pi 3 is 17 for IR Transmitter and GPIO output pin is 27 for IR Receiver.

5. Type the following command to edit `hardware.conf` file:

```
sudo leafpad /etc/lirc/hardware.conf
```

6. Change `hardware.conf` file exactly as the following file

```
#####
# /etc/lirc/hardware.conf
#
# Arguments which will be used when launching lircd
LIRCD_ARGS="--uinput"
# Don't start lircmd even if there seems to be a good config
file
# START_LIRC_CMD=false
# Don't start irexec, even if a good config file seems to exist.
# START_IEXEC=false
# Try to load appropriate kernel modules
LOAD_MODULES=true
# Run "lircd --driver=help" for a list of supported drivers.
DRIVER="default"
# usually /dev/lirc0 is the correct setting for systems using
udev
DEVICE="/dev/lirc0"
MODULES="lirc_rpi"
# Default configuration files for your hardware if any
LIRCD_CONF=""
LIRC_CMD_CONF=""
#####
```

7. Type the following commands to stop and start *lircd* service so that the above made changes take effect successfully:

```
sudo /etc/init.d/lirc stop
sudo /etc/init.d/lirc start
```

8. Type the following command to edit *config.txt* file:

```
sudo leafpad /boot/config.txt
```

9. Add the following line into *config.txt* file:

```
dtoverlay=lircrpi,gpio_in_pin=17,
gpio_out_pin=7
```

10. Type the following command to reboot your Raspberry Pi 3 in order to save changes made above:

```
sudo reboot
```

h) *IR Receiver*

i. *Wiring up IR Receiver*

1. Place IR Receiver in your solder less bread board.
 2. The data pin is connected to GPIO pin 27 as per the configuration we made earlier in LIRC.
 3. The ground pin is connected to GPIO ground pin in your Raspberry Pi 3.
 4. The +5v pin is connected to GPIO 5v pin (DC Power) in your Raspberry Pi 3 in order to power on your IR Receiver.
- ❖ *Note:* Data pin and +5v in your IR Receiver vary from type to type. You are recommended to review

data sheet of the IR Receiver you decide to use. In this project, I used the data sheet of the IR Receiver I used and listed in LIST of FIGURES Section (Page 7).

ii. *Testing the IR Receiver Circuit*

1. Power on your Raspberry Pi 3.
2. Open the terminal in your Raspberry Pi 3 and type the following command to stop *lircd* service:

```
sudo /etc/init.d/lirc stop
```

3. Type the following command to start outputting raw data received from IR Receiver:

```
mode2 -d /dev/lirc0
```

4. Point your air conditioner remote control to the IR receiver you wired up earlier and start pressing the buttons. If your output in the terminal looks as the following:

```
space 16300
pulse 95
space 28794
pulse 80
space 19395
pulse 83
space 402351
pulse 135
space 7085
pulse 85
space 2903
```


It means your IR Receiver circuit is implemented and configured properly.

i) IR Transmitter

i. Wiring up IR Transmitter

1. Place IR Transmitter in your solder less bread board.
2. Place NP2222 transistor in series with the IR Transmitter (short pin of the IR Transmitter).

- ❖ *Note:* The main function of the NP2222 transistor is amplifying or/and switching electronic signals and electrical power. In other words, any applied current or voltage to one pair of the transistor may be changed before reaching the other pair of the transistor as needed.
3. Place 10k ohm resistor in series with the NP2222 transistor, one pin in series with the base and one pin in series with the collector.

- ❖ *Note:* The main function of the 10k ohm resistor is to control the current flows across the IR Transmitter and keep it safe from burning.

4. The long pin of the IR Transmitter is connected to GPIO 5v pin (DC Power) in your Raspberry Pi 3 in order to power on your IR Transmitter.
5. The first pin of 10k ohm resistor that is connected in series with NP2222 transistor is connected to GPIO pin 17 as per the configuration we made earlier in LIRC.
6. The second pin of 10k ohm resistor is connected to GPIO ground pin in your raspberry Pi 3.

ii. Testing the IR Transmitter Circuit

1. Power on your Raspberry Pi 3.
2. Open the terminal in your Raspberry Pi 3 and type the following command to stop *lircd* service:
`sudo /etc/init.d/lirc stop`



Figure 21: Screenshot of lircd command on terminal window

Create a new configuration file for your air conditioner remote control called *ir1.conf* using the following command:

```
irrecord -d /dev/lirc0 -f ir1.conf
```



Figure 22: Screenshot of creating new configuration file on Raspbian



Then you are supposed to get message as shown in figures below to start recording your air conditioner remote control codes:

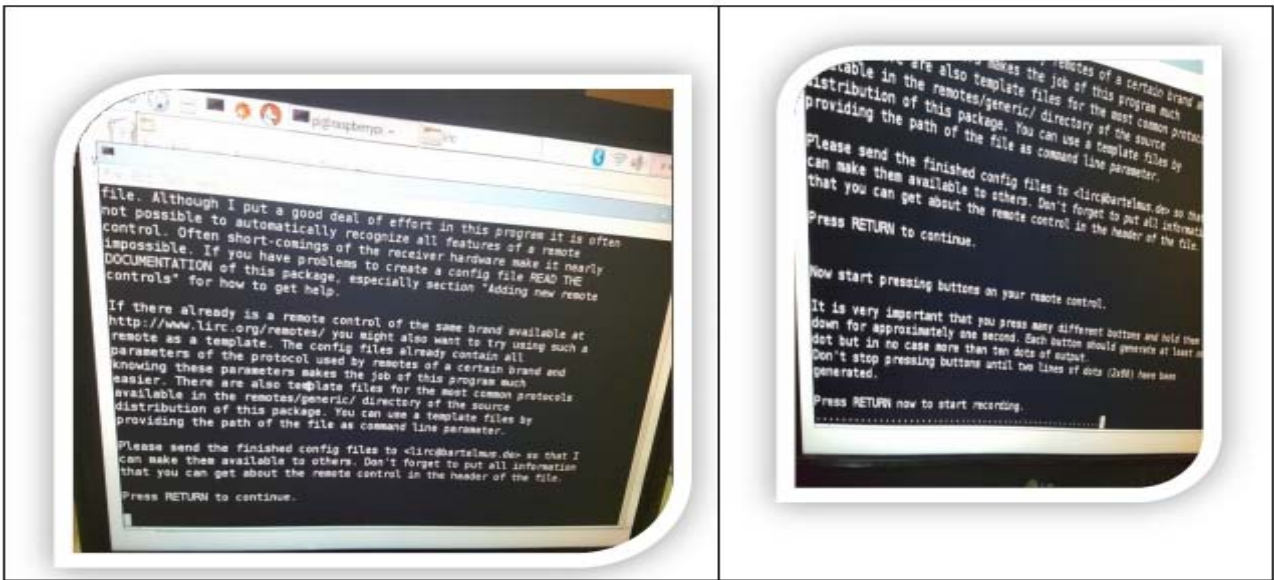


Figure 23: Screenshots of irrecod instructions

You have to follow the instruction and record codes to turn on, turn off, increase the volume of the temperature and decrease the volume of the temperature for the air conditioner.

Then you will be prompt to enter a name for each button you press. Kindly, note that you cannot

enter any random names for your recorded keys. LIRC has its own buttons' names. In order to check these valid names, type the following command:

```
irrecord --list-namespace
```

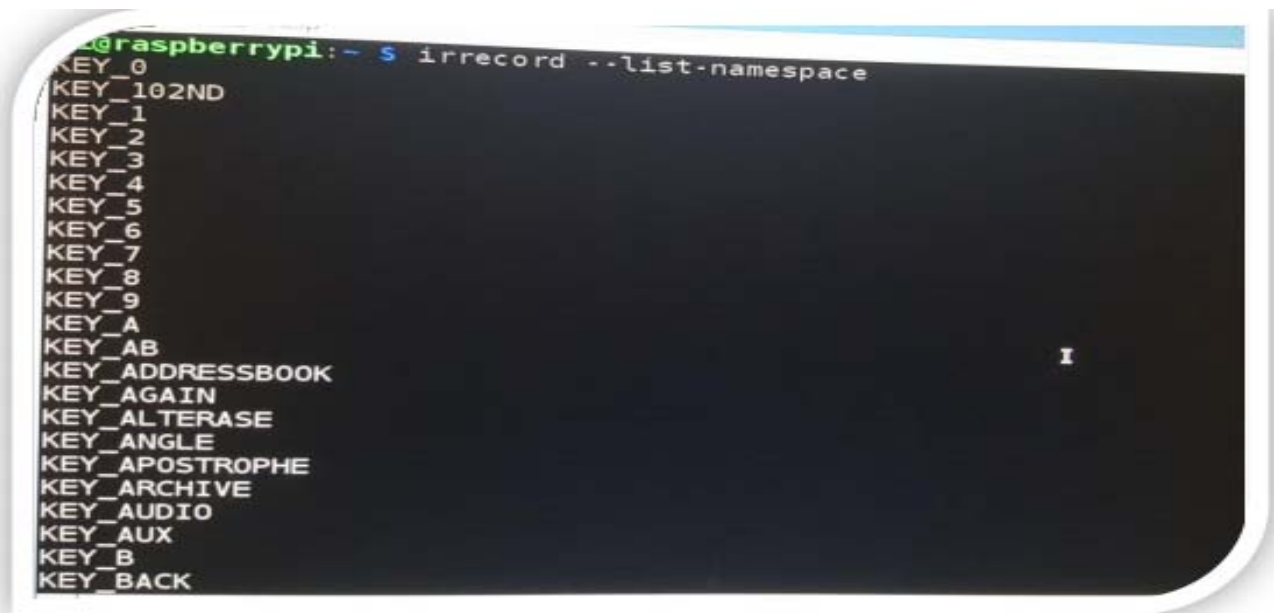


Figure 24: Screenshots of valid names assigned to recorded buttons in LIRC

In this test I picked up the following keys

- KEY_POWER to turn on the air conditioner.
- KEY_POWER2 to turn off the air conditioner.

- KEY_UP to increase the volume of the temperature.
- KEY_DOWN to decrease the volume of the temperature.

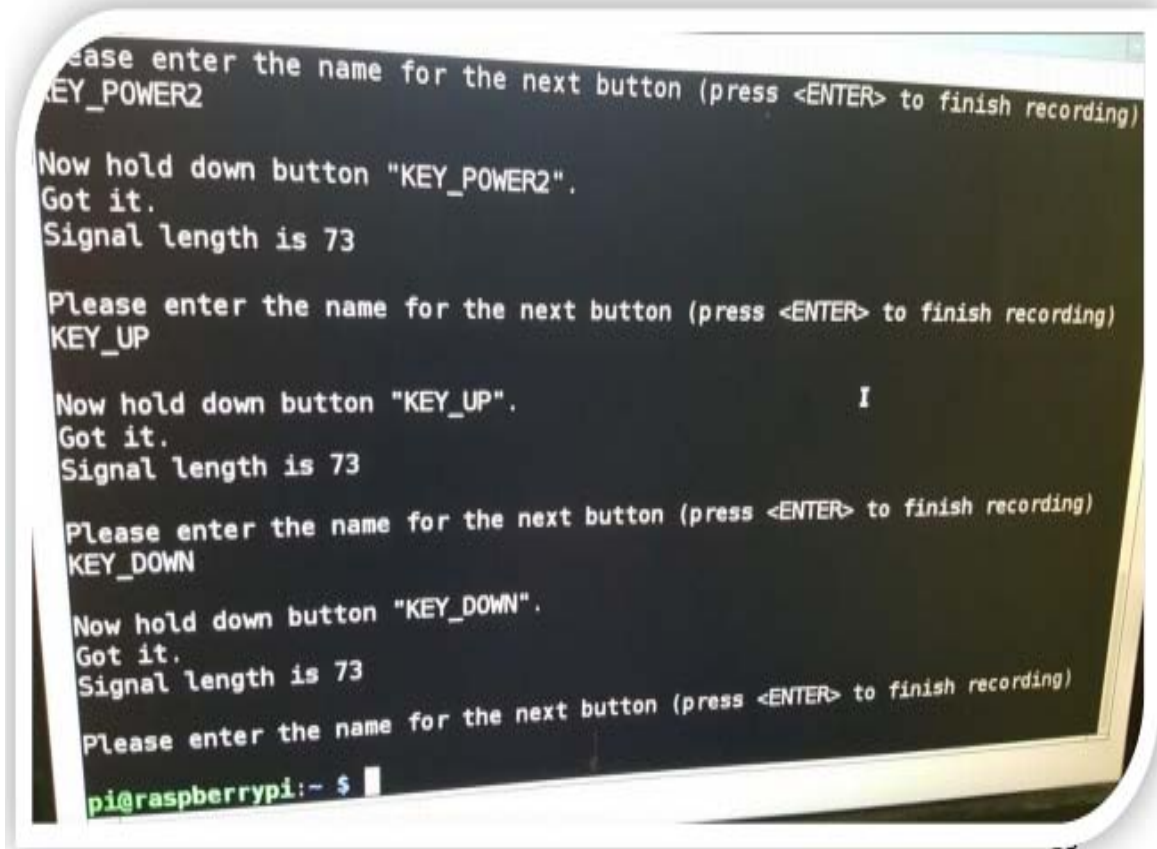


Figure 25: Screenshot of assigning names to recorded buttons

3. Copy the new created *ir1.conf* file into the original *lircd.conf* file created by LIRC using the command:


```
sudo cp ir1.conf /etc/lirc/lircd.conf
```
4. Type the following command to start *lircd* service:


```
sudo /etc/init.d/lirc start
```
5. In order to send the recorded signal for turning on the air conditioner that is saved in *lircd.conf*, type the following command:


```
irsend SEND_ONCE ir1.conf KEY_POWER
```



Figure 26: Screenshot of switching air conditioner in command window

6. In order to send the recorded signal for turning off the air conditioner that is saved in *lircd.conf*, type the following command:


```
irsend SEND_ONCE ir1.conf KEY_POWER2
```
7. In order to send the recorded signal for increasing the volume of the temperature, type the following command:


```
irsend SEND_ONCE ir1.conf KEY_UP
```

8. In order to send the recorded signal for decreasing the volume of the temperature, type the following command:

```
irsend SEND_ONCE ir1.conf
      KEY_DOWN
```

If your air conditioner turns on and off, increases and decreases the volume of the temperature successfully, it means your IR Transmitter circuit is implemented and configured properly.

j) *PIR Sensor*

i. *Wiring up PIR Sensor*

1. Place PIR Sensor in your solder less bread board.
2. The input pin is connected to GPIO pin 04 in your Raspberry Pi 3.
3. The output pin is connected to GPIO pin 27 in your Raspberry Pi 3.
4. The +5v pin is connected to GPIO 5v pin (DC Power) in your Raspberry Pi 3 in order to power on your PIR Sensor.

ii. *Programming PIR Sensor*

- ❖ *Note:* Python programming language will be used to program PIR Sensor.

1. Type the following command to create *pir.py* file:

```
sudo nano pir.py
```

2. Write the following Python code inside *pir.py* file:

See APPENDIX B: IMPLEMENTATION SOURCE CODE, Section I: PIR Sensor Source Code

iii. *Testing the PIR Sensor Circuit*

- ❖ *Note:* For testing purposes, I have changed time period to sense any motion before switching off the air conditioner into 10 seconds. In my real project, I set time period to 1800 seconds.

1. Power on your Raspberry Pi 3.
2. Type the following command to start *lircd* service:

```
sudo /etc/init.d/lirc start
```

3. Type the following command to start your PIR Sensor:

```
sudo python /home/pi/pir.py
```

Now you will see that PIR Sensor is working, if you move your hand in front of the PIR Sensor circuit, you will see number 1 displays in your terminal.

Number 1 means that PIR Sensor detects a motion. Now remove your hand and stay stable for 10 seconds, you will notice number 0 displays in the terminal. Number 0 means that PIR Sensor does not detect any motion.

Wait for 10 seconds and if your air conditioner turned off then, your PIR Sensor circuit is implemented and configured successfully.

k) *Web Application Development*

i. *Developing Web Application*

- ❖ *Note 1:* PHP web language is used to create the web page.

MySQL database engine is used to create the database.

PHP web language is used as connection agent between the web page and the database.

- ❖ *Note 2:* All files related to the web application development will be found the following path:

```
/var/www/html
```

ii. *Creating the Web Page*

1. Open the terminal in your Raspberry Pi 3.
2. Type the following command to access */var/www/html* directory:

```
cd /var/www/html
```

3. Type the following command to create *iotAC.php* file:

```
sudo touch iotAC.php
```

4. Type the following command to give full permission to *iotAC.php* file while editing:

```
sudo chmod 777 iotAC.php
```

5. Go to */var/www/html* directory and double click on *iotAC.php* you have created in step 3.

6. Add the following PHP code and save the file: See APPENDIX B: IMPLEMENTATION SOURCE CODE, Section II: *iotAC.php* Source Code

iii. *Building up the Database*

1. Open the terminal in your Raspberry Pi 3.
2. Type the following command to access MySQL server:

```
mysql -u root -p
```

It will prompt you to enter the password you have created when you setup MySQL server earlier in this Chapter. In my project, my password is: mysql

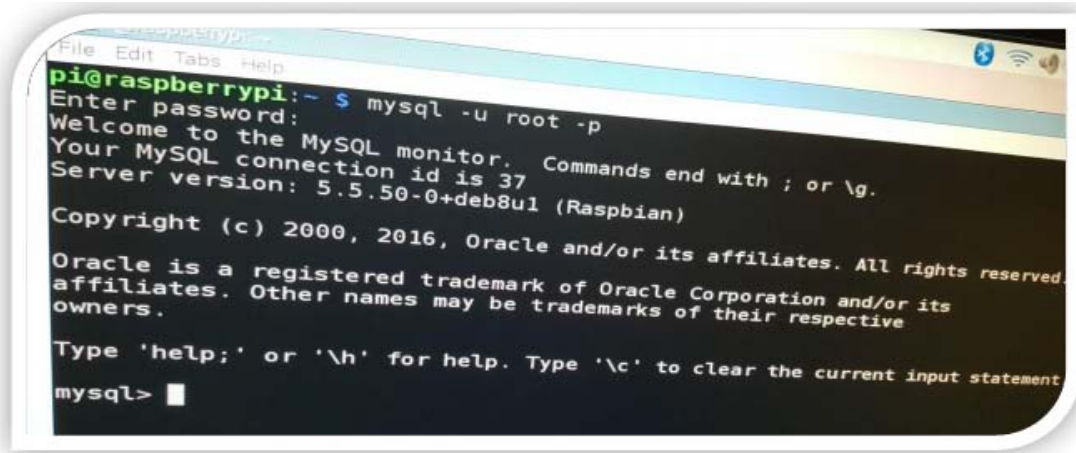


Figure 27: Screenshot of establishing MySQL server connection

3. Type the following command to show the databases you have in your server



Figure 28: Screenshot of displaying databases available in MySQL

4. Type the following command to create a new database called *ac_control*: the *ac_control* database you have created in step 4 is among them:

```
CREATE DATABASE ac_control;
SHOW DATABASES
```

7. Type the following command to show the databases you have in your server and make sure that



Figure 29: Screenshot of creating a new database in MySQL



8. Type the following command to access `ac_control` database:

```
USE ac_control;
```

9. Type the following command to create a table inside `ac_control` database called `login` which have username and password parameters:

```
CREATE TABLE `login` (`username`
  VARCHAR (255), `password`
  VARCHAR(255))
```

10. Type the following command to add master username with `master-ac@321` password into `login` table inside `ac_control` database:

```
INSERT INTO login values
  (`master`,`master-ac@321`)
```

11. Type the following command to check if the username and password you have added in step 8 exist in `login` table:

```
SELECT * FROM login
```

12. Type the following command to quit MySQL server:

```
pi@raspberrypi:~$ mysql
mysql>
mysql> use ac_control
Database changed
mysql> INSERT INTO login values('master','master-ac@321');
Query OK, 1 row affected (0.02 sec)

mysql> SELECT * FROM ac_control;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
corresponds to your MySQL server version for the right syntax to use near
'rol' at line 1
mysql> SELECT * FROM login;
+-----+-----+
| username | password |
+-----+-----+
| master   | master-ac@321 |
+-----+-----+
1 row in set (0.00 sec)

mysql> quit;
Bye
pi@raspberrypi:~$
```

Figure 30: Screenshot of different queries to `ac_control` database in MySQL

l) Login Web Page

- ❖ Note: In order to make my web application secure, I have created a login web page.

1. Open the terminal in your Raspberry Pi 3.
2. Type the following command to access `/var/www/html` directory:

```
cd /var/www/html
```

3. Type the following command to create `login.php` file:

```
sudo touch login.php
```

4. Type the following command to give full permission to `login.php` file while editing:

```
sudo chmod 777 login.php
```

5. Go to `/var/www/html` directory and double click on `login.php` you have created in step 3.
6. Add the following PHP code and save the file:

See APPENDIX B: IMPLEMENTATION SOURCE CODE, Section II: `login.php` Source Code

m) Connection between Login Web Page and `ac_control` Database

- ❖ Note1: In order to connect between login web page and `ac_control` database, I have created a PHP file called `submit`.

1. Open the terminal in your Raspberry Pi 3.
2. Type the following command to access `/var/www/html` directory:

```
cd /var/www/html
```

3. Type the following command to create `submit.php` file:

```
sudo touch header.php
```

4. Type the following command to give full permission to `submit.php` file while editing:

```
sudo chmod 777 header.php
```

5. Go to `/var/www/html` directory and double click on `submit.php` you have created in step 3.
6. Add the following PHP code and save the file:

See APPENDIX B: IMPLEMENTATION SOURCE CODE, Section IV: `submit.php` Source Code

n) Creating PHP file that contains Required Credentials to Connect to MySQL

Server:

- ❖ Note: In order for the `submit.php` file to connect to MySQL server, `header.php` file must be created to contain all required credentials.

1. Open the terminal in your Raspberry Pi 3.
2. Type the following command to access `/var/www/html` directory:

```
sudo /etc/init.d/lirc start
```
3. Type the following command to create `header.php` file:

```
sudo touch header.php
```
4. Type the following command to give full permission to `header.php` file while editing:

```
sudo chmod 777 header.php
```
5. Go to `/var/www/html` directory and double click on `header.php` you have created in step 3.
6. Add the following PHP code and save the file:

See APPENDIX B: IMPLEMENTATION SOURCE CODE, Section V: `header.php` Source Code

o) Testing Web Application

First: Testing Web Application when the Raspberry Pi 3 and Web Browser Device belong to the same network:

1. Power on your Raspberry Pi 3.
2. Connect your Raspberry Pi 3 to Wi-Fi through wireless dongle.

3. Open the terminal in Raspberry Pi 3 and type the following command to start `lircd` service:

```
sudo /etc/init.d/lirc start
```
4. Type the following command to start your PIR Sensor:

```
sudo python /home/pi/pir.py
```
5. Open the browser in your Raspberry Pi 3 and type the following:

`http://the IP address of your Raspberry Pi3/login.php`

In order to check the IP address of the Raspberry Pi, type the following command:

`ifconfig`

In my project, the IP address of my Raspberry Pi 3 is: 192.168.43.181, so it will be something like:

`http://192.168.43.181/login.php`

6. Insert the username: `master` and the password: `master-ac@321` and click `Submit` button. You should be directed to `iotAC.php` page. Now click `ON` to turn on the air conditioner, `OFF` to turn off the air conditioner, `+` to increase temperature volume and `-` to decrease temperature volume. If all buttons operate as it is supposed, then your application is developed successfully.



Figure 31: Login Page of air conditioner website

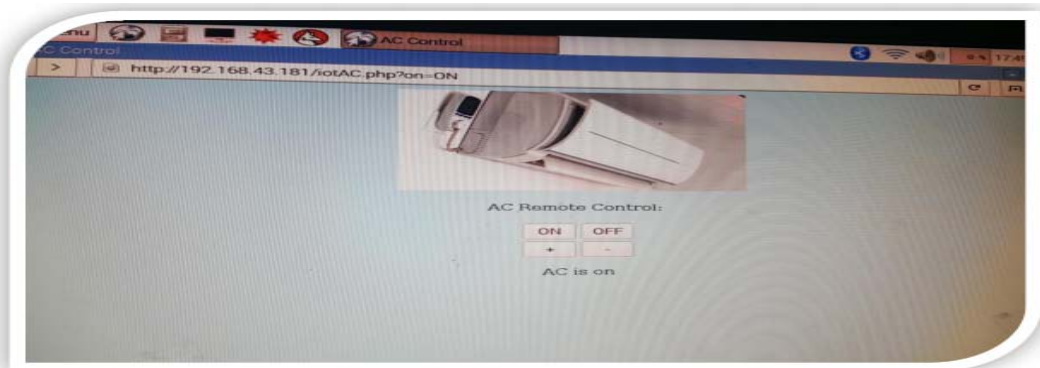


Figure 32: Air conditioner webpage



Note 1: If the user forgot to insert the username, the password or both of them, an error message is displayed.

7. Repeat steps 5 and 6 but with any device (desktop, laptop, PDA and smart phone) connected to the same local network as the Raspberry Pi 3.

❖ Note 2: It is not practical to run *lircd* service and *pir.py* service each time. As a result, I will configure

them to start automatically when Raspberry Pi starts up.

1. Open terminal in Raspberry Pi 3.
2. Type the following command to open crontab editor:

```
sudo crontab -e
```



Figure 33: Screenshot of executing crontab editor

3. Add the following lines and exit the editor:

```
@reboot sudo /etc/init.d/lirc start &
@reboot sudo python /home/pi/pir.py &
```

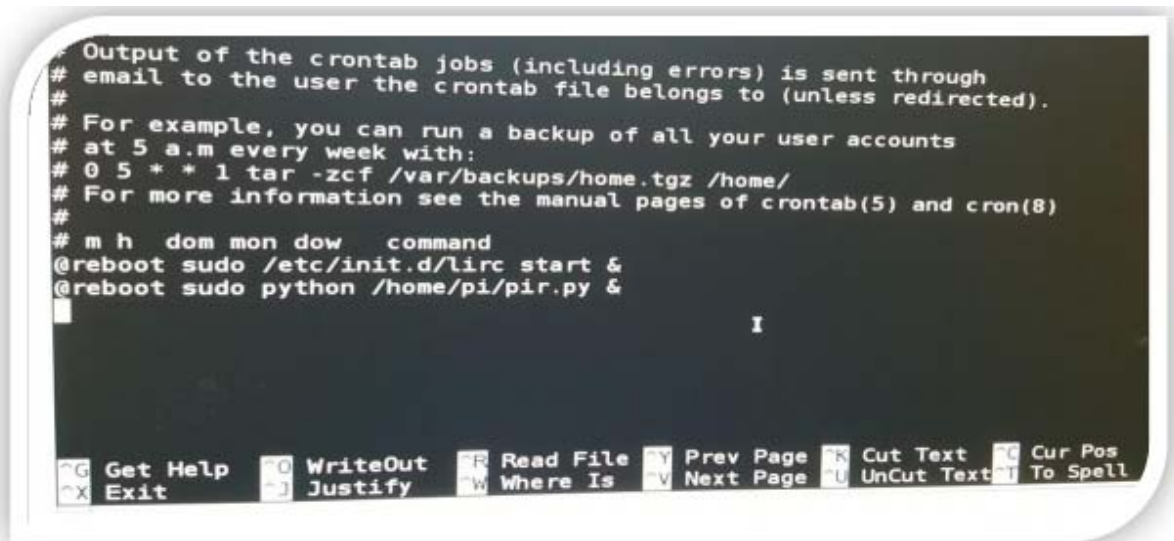


Figure 34: Screenshot of crontab editor

4. Press `ctrl + x` to exit the editor and press `Y` when it prompts you to save changes using `CTRL + X`

❖ Note 3: It is not practical for the Raspberry Pi IP address to keep changes automatically.

As a result, I will configure both Wireless and Ethernet interfaces to have a static IP address in my Raspberry Pi 3.

1. Open terminal in Raspberry Pi 3.
2. Type the following command to edit *dhcpcd.conf* file:

```
sudo nano /etc/dhcpcd.conf
```

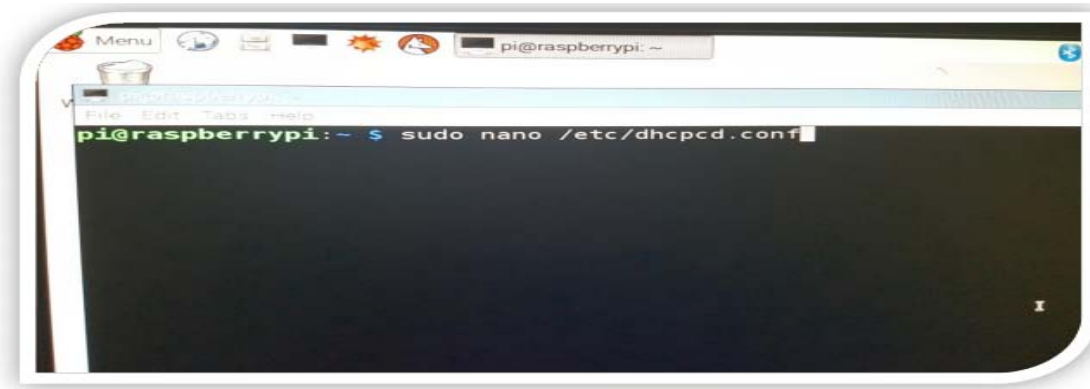


Figure 35: Screenshot of editing dhcpd.conf file using nano text editor

3. Add the following parameters under interface eth0:

```
static ip_address=192.168.43.181/24
static routers=192.168.43.1
static domain_name_servers=192.168.43.1
```
4. Add the following parameters under wlan0:

```
static ip_address=192.168.43.181/24
static routers=192.168.43.1
static domain_name_servers=192.168.43.1
```

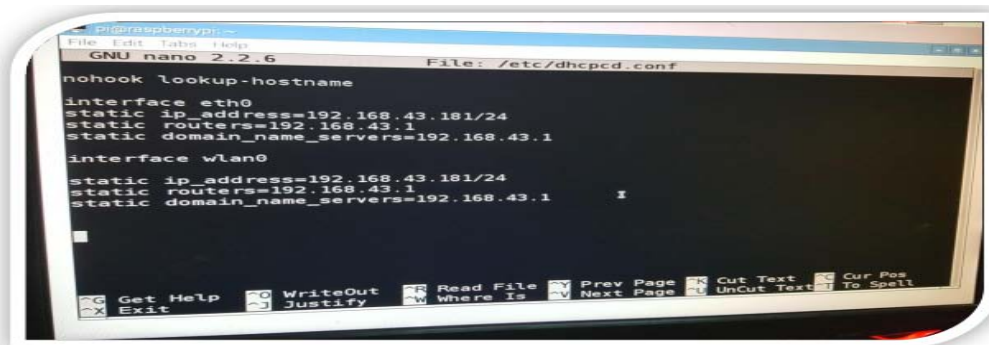


Figure 36: Screenshot of dhcpd.conf

5. Press `ctrl + x` to exit the editor and press `Y` when it prompts you to save changes using `CTRL + X`
6. Reboot your Raspberry Pi 3 in order to take effect of made changes using the command:

```
sudo reboot
```
7. Check the IP address of the Raspberry Pi by type the following command:

`Ifconfig`

- p) *Accessing Developed Web Application from Anywhere Over the Internet*
- ❖ *Note 1:* The developed web application is implanted and tested successfully as it discussed above. However, any user can control the air conditioner remotely within the local network only. In order to be able to control the air conditioner from the internet outside your local network, you need a public IP address for your Raspberry Pi 3. In this project, I used Weaved services.

Weaved is a free software to be installed in Raspberry Pi and enables the user to connect to this Raspberry Pi and access its hosted web pages over internet from anywhere. In fact, Weaved provides Internet of Things (IOT) Kit to be used in Raspberry Pi. Weaved offers many services such as: SSH on port 22, Web (HTTP) on port 80, VNC on port 5901 and custom TCP connection (Sangesari, 2015).

- q) *Setting Up Weaved Software in Raspberry Pi 3:*

1. Create a free account in Weaved website:
<https://developer.weaved.com/portal/index.php>
2. Power on your Raspberry Pi 3.
3. Connect your Raspberry Pi 3 to Wi-Fi.
4. Open terminal in your Raspberry Pi 3.
5. Type the following command to download Weaved software package using `wget` utility:

```
wget
https://github.com/weaved/installer/raw/master/binaries/
weaved-nixinstaller_1.2.13.bin
```

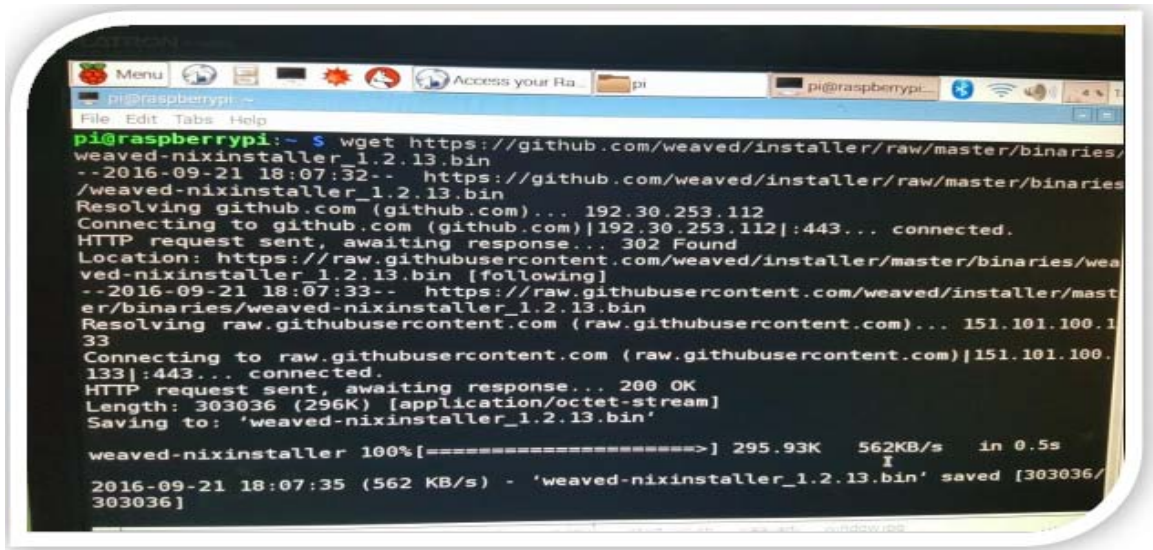


Figure 37: Screenshot of downloading weaved installer using wget utility

6. Type the following command to make the installer executable:


```
chmod +x weaved-nixinstaller_1.2.13.bin
```
7. Type the following command to launch the executable installer:


```
./weaved-nixinstaller_1.2.13.bin
```
8. Select the service you want from the listed services. In my project I select:
 - Web (HTTP) on default port 80
 - ❖ *Note 1:* You will be asked in you want to continue with the default assigned port which is 80. If you decide to keep it the same as default, type y. If you decide to change the port, type n and follow the instructions. In my project, I chose to keep the default port 80.

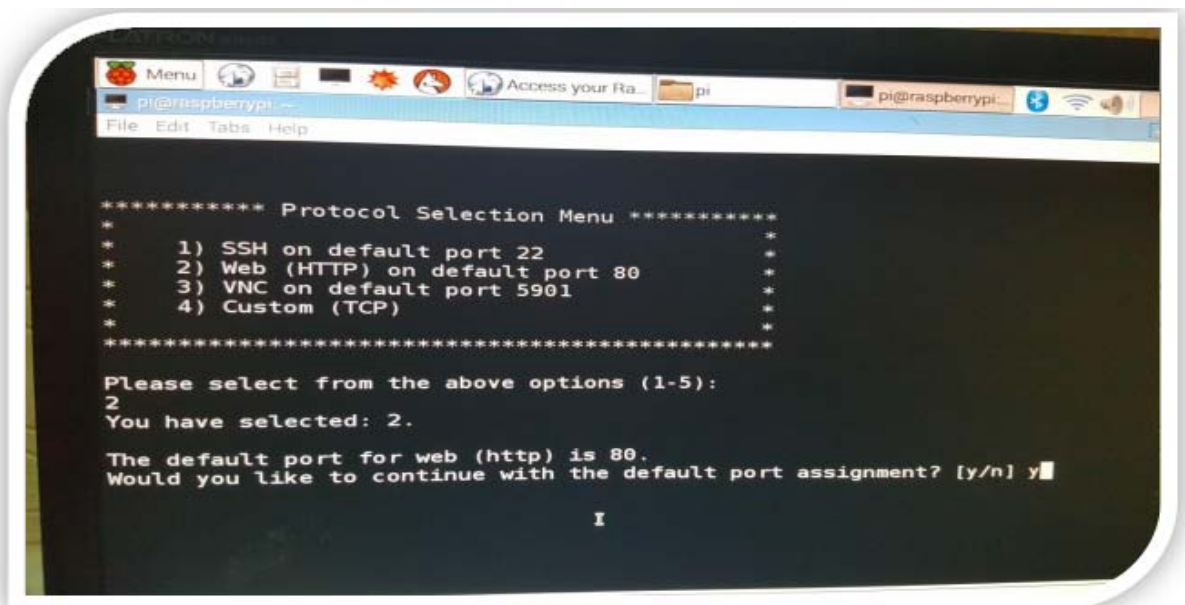


Figure 38: Select the required weaved service

9. Enter your username which is the email address you have created in step 1 above.
10. Enter your password for your username.



```
Please select from the above options (1-5):
2
You have selected: 2.

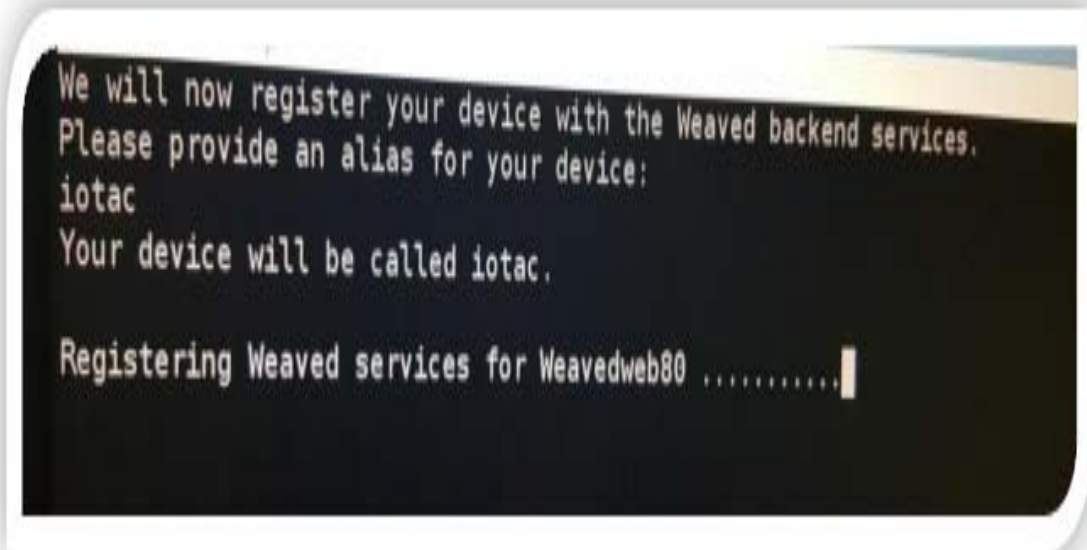
The default port for web (http) is 80.
Would you like to continue with the default port assignment? [y/n] y
We will install Weaved services for the following:

Protocol: web
Port #: 80
Service name: Weavedweb80

Please enter your Weaved Username (email address):
kholood.alsaidi@gmail.com
Now, please enter your password:
```

Figure 39: Login details for waved web services

- ❖ Note 2: You will be asked to enter an alias for your device, type the name you admire. In my project, I typed: *iotac*



```
We will now register your device with the Weaved backend services.
Please provide an alias for your device:
iotac
Your device will be called iotac.

Registering Weaved services for Weavedweb80 .....
```

Figure 40: Register the device with Weaved backend service

11. Wait until installation is done.

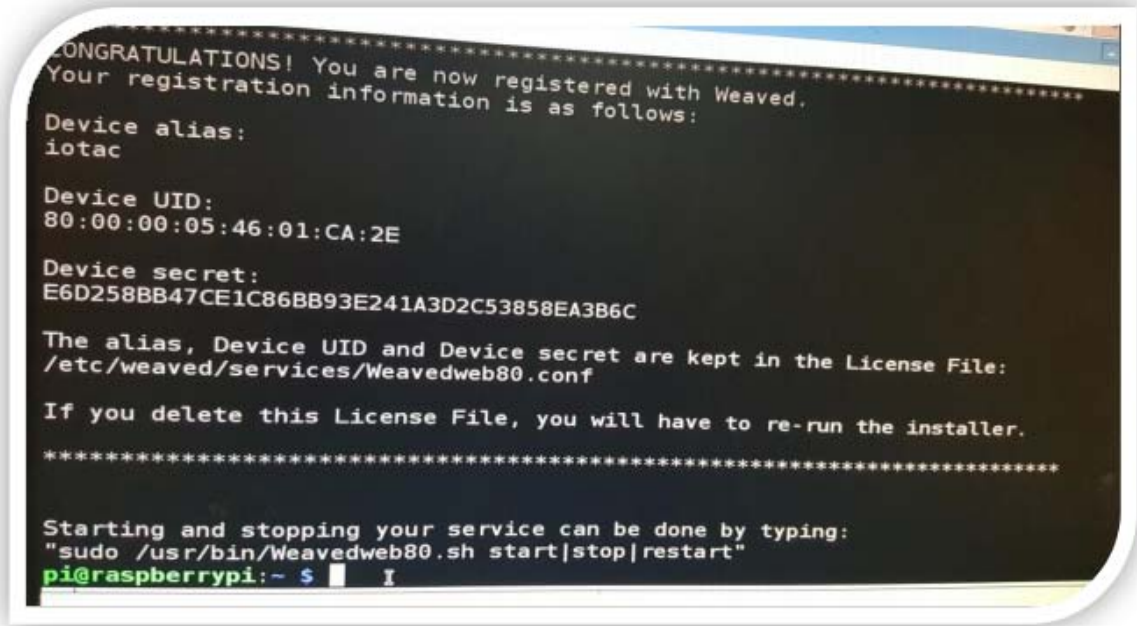


Figure 41: Screenshot of weaved web installation

12. Sign into your Weaved service in the following link:
<https://developer.weaved.com/portal/login.php?error=NoSession>

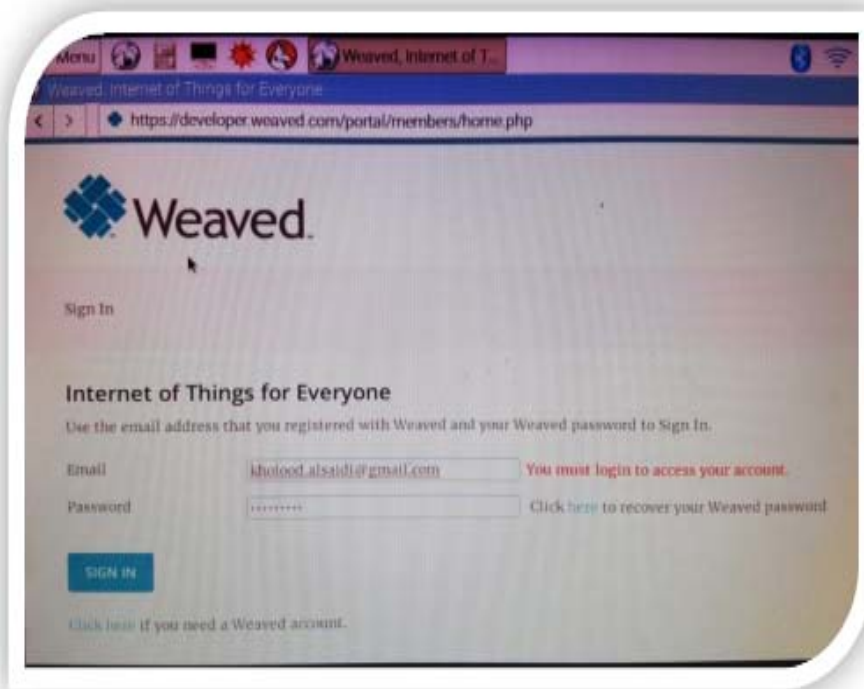


Figure 42: Login Page of Weaved service

13. Navigate to Your current list of services, you must be able to see that your selected service is listed as shown

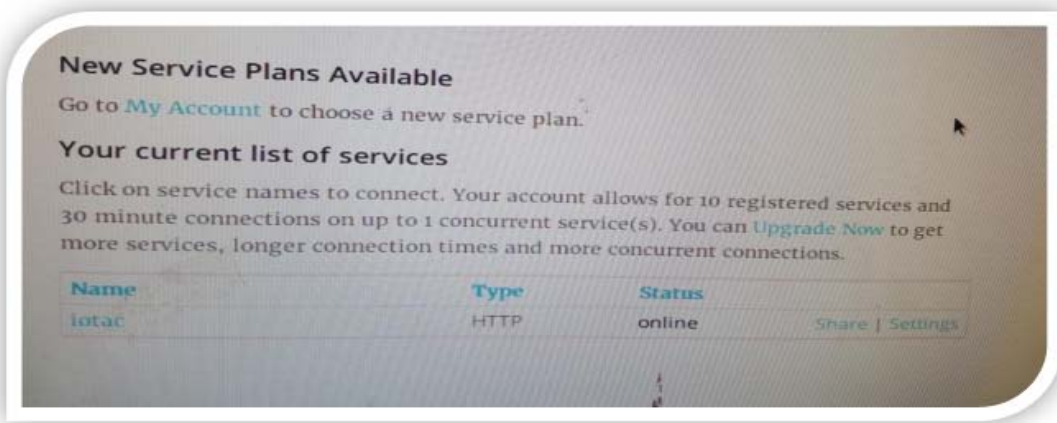


Figure 43: Weaved service page

- Click on the *alias* for your services listed under Name column in order to connect your service. Then your service settings will be displayed.



Figure 44: IP address to connect to service

- When your service is connected it will display apache server web page says It works! It means your service is up now. Take the address after `http://` and paste it in your web browser with the name of your web page in your Raspberry Pi3. In my project: `pjgwefdz.p6.weaved.com` is the address of after `http://`



Figure 45: Apache2 Debian Default Page

16. I opened my web browser and typed the following in the address bar:

`http:// pjpgwfdz.p6.weaved.com/login.php`

❖ *Note 3:* Note that each time you connect to your service; the address is going to be different. It is not practical from one side but from the other side you may consider this as a security in case of any hacker eaves-dropped your address.

❖ *Note 4:* It is not practical to run Weaved service each time. As a result, I will configure it to start automatically when Raspberry Pi starts up.

1. Open terminal in Raspberry Pi 3.
2. Type the following command to open crontab editor:

```
sudo crontab -e
```

3. Add the following lines and exit the editor:

- ```
@reboot sudo
/usr/bin/Weavedweb80.sh start &
```
4. Press ctrl + x to exit the editor and press Y when it prompts you to save changes using CTRL + X
  5. Reboot your Raspberry Pi 3 in order to take effect of made changes using the command:

```
sudo reboot
```

## V. INTEGRATION AND TESTING

### a) Integration

Now implementing and configuring each circuit was done successfully. The second stage of implementation is integration. Integration means combining all individual circuits in one solderless bread board in order to create one complete circuit. The integrated circuit is illustrated in Figure11.

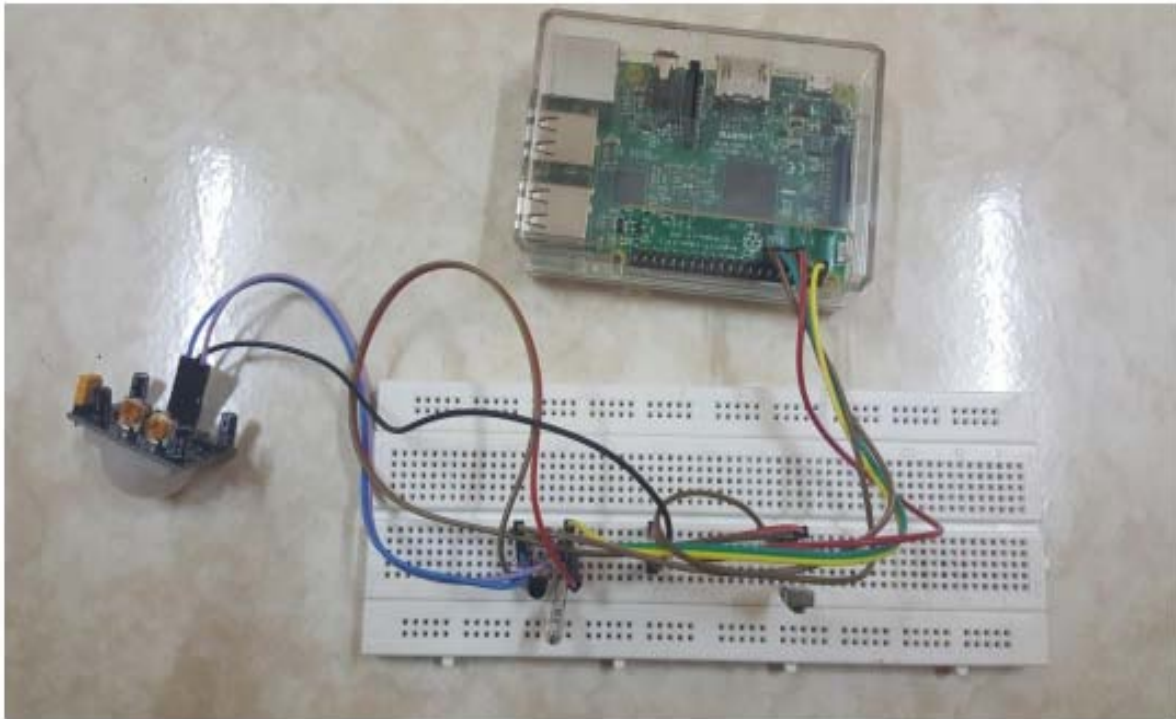


Figure 46: Smart Air Conditioner Using Internet of Things Integrated Circuit

### Testing:

Same testing techniques used in Section 4.3 Implementation and Testing can be applied in the integrated circuit. If same results are obtained, then your integration is done properly.

Results are discussed and illustrated in details in 4.5 Results Section.

### b) Results

After implementing the smart air conditioner project successfully, the following figures illustrate the results of the project tested and carried out by a smart

phone which does not belong to the same network the Raspberry Pi 3 is connected to. It means, the smart phone is somewhere away from the Raspberry Pi 3 network and they are connected over the internet using Weaved service.



Figure 47: login.php Web Page



Figure 48: Login Credentials



Figure 49: iotAC.php Web Page



Figure 50: The Air Conditioner is Turned Off

VI. CONCLUSION

a) Evaluation

In order to validate the implemented smart air conditioner, a questionnaire was conducted by 14 potential users. The collected results were analyzed using IBM SPSS Statistics software. IBM SPSS Statistics

1. I am interested on home automation services. Statistics I am interested on home automation services.

is a famous data analysis software package. It helps the user to address his/her analytical process starting from planning and collecting data, moving to analyzing, reporting and deploying data (IBM, 2016).

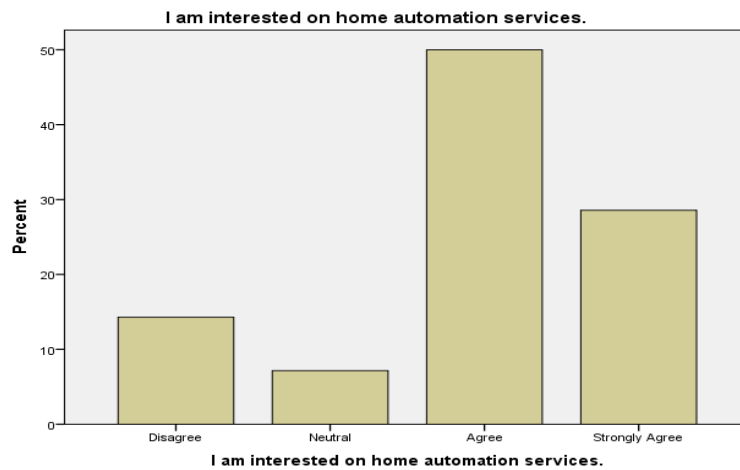
The followings are the obtained statistics per each question raised in the questionnaire.

|         |         |                     |
|---------|---------|---------------------|
| N       | Valid   | 14                  |
|         | Missing | 0                   |
| Mean    |         | 3.9286              |
| Median  |         | 4.0909 <sup>a</sup> |
| Maximum |         | 5.00                |

a. Calculated from grouped data.

I am interested on home automation services.

|                | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------|-----------|---------|---------------|--------------------|
| Valid Disagree | 2         | 14.3    | 14.3          | 14.3               |
| Neutral        | 1         | 7.1     | 7.1           | 21.4               |
| Agree          | 7         | 50.0    | 50.0          | 71.4               |
| Strongly Agree | 4         | 28.6    | 28.6          | 100.0              |
| Total          | 14        | 100.0   | 100.0         |                    |



2. The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

*Statistics*

The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

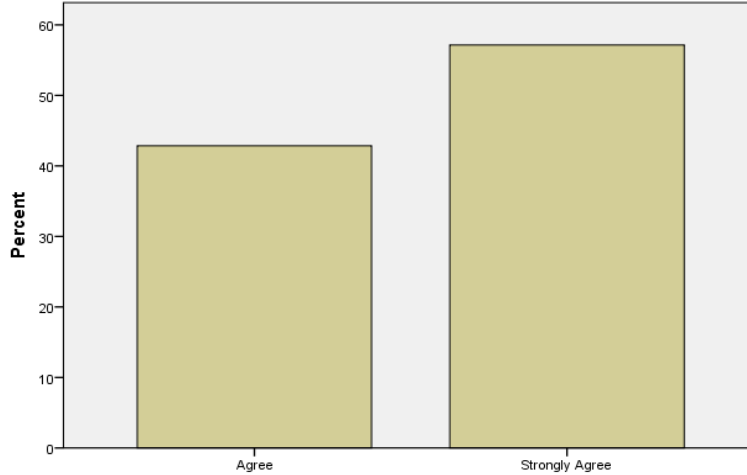
|         |         |                     |
|---------|---------|---------------------|
| N       | Valid   | 14                  |
|         | Missing | 0                   |
| Mean    |         | 4.5714              |
| Median  |         | 4.5714 <sup>a</sup> |
| Maximum |         | 5.00                |

a. Calculated from grouped data.

The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

|                | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------|-----------|---------|---------------|--------------------|
| Valid Strongly | 6         | 42.9    | 42.9          | 42.9               |
| Total          | 8         | 57.1    | 57.1          | 100.0              |
| Total          | 14        | 100.0   | 100.0         |                    |

The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.



The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

3. The system is easy to use.

*Statistics*

*The system is easy to use.*

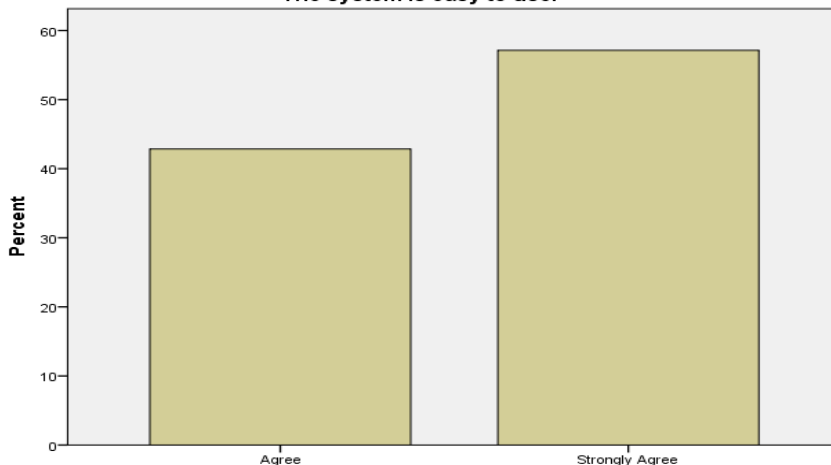
|         |         |                     |
|---------|---------|---------------------|
| N       | Valid   | 14                  |
|         | Missing | 0                   |
| Mean    |         | 4.5714              |
| Median  |         | 4.5714 <sup>a</sup> |
| Maximum |         | 5.00                |

a. Calculated from grouped data.

*The system is easy to use.*

|                      | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|--------------------|
| Agree                | 6         | 42.9    | 42.9          | 42.9               |
| Valid Strongly Agree | 8         | 57.1    | 57.1          | 100.0              |
| Total                | 14        | 100.0   | 100.0         |                    |

The system is easy to use.



The system is easy to use.





4. I feel much more comfortable to use this system than the local remote control.

*Statistics*

I feel much more comfortable to use this system than the local remote control

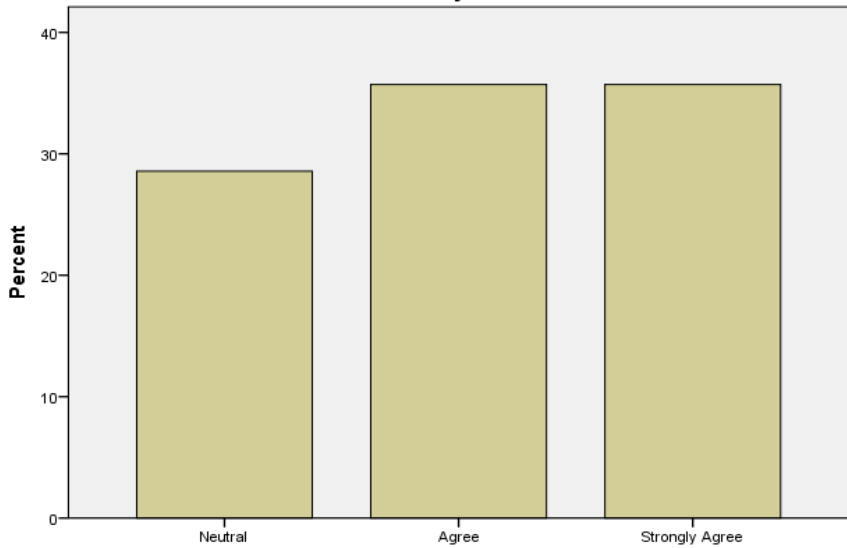
|         |         |                     |
|---------|---------|---------------------|
| N       | Valid   | 14                  |
|         | Missing | 0                   |
| Mean    |         | 4.0714              |
| Median  |         | 4.1000 <sup>a</sup> |
| Maximum |         | 5.00                |

a. Calculated from grouped data.

I feel much more comfortable to use this system than the local remote control.

|                | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------|-----------|---------|---------------|--------------------|
| Neutral        | 4         | 28.6    | 28.6          | 28.6               |
| Agree          | 5         | 35.7    | 35.7          | 64.3               |
| Strongly Agree | 5         | 35.7    | 35.7          | 100.0              |
| Total          | 14        | 100.0   | 100.0         |                    |

I feel much more comfortable to use this system than the local remote control.



I feel much more comfortable to use this system than the local remote control.

5. I recommend using this system as a product in technology market.

*Statistics*

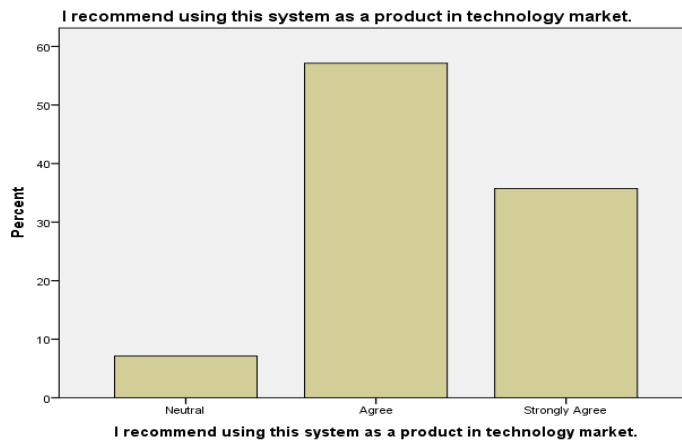
I recommend using this system as a product in technology market.

|         |         |                     |
|---------|---------|---------------------|
| N       | Valid   | 14                  |
|         | Missing | 0                   |
| Mean    |         | 4.2857              |
| Median  |         | 4.3077 <sup>a</sup> |
| Maximum |         | 5.00                |

a. Calculated from grouped data.

I recommend using this system as a product in technology market.

|       | Frequency      | Percent | Valid Percent | Cumulative Percent |
|-------|----------------|---------|---------------|--------------------|
| Valid | Neutral        | 1       | 7.1           | 7.1                |
|       | Agree          | 8       | 57.1          | 64.3               |
|       | Strongly Agree | 5       | 35.7          | 35.7               |
|       | Total          | 14      | 100.0         | 100.0              |



Through reviewing the above obtained statistics, the implemented smart air conditioner product is obviously gaining trust of the potential users and accordingly the gained features from the implemented product are: The smart air conditioner has absolutely no inference against real remote control. The product is cost effective, energy efficient and achieves automation functionality indeed.

b) Summary

The local remote control is the traditional mechanism in which the end user controls the air conditioner. In the absence of this mechanism, the user loses the control. However, there is another mechanism in which the user may remotely control the air conditioner through Internet of Things (IoT) technology. A smart air conditioner using IoT was designed and implemented using Raspberry Pi 3 Model B device. Validity of the project was achieved through testing the implemented product by 14 potential users who own SANYO air conditioner. All potential users were able to control their air conditioner remotely over the internet from anywhere. The smart air conditioner has absolutely no inference against real remote control. The product is

cost effective, energy efficient and achieves the required automation functionality.

c) Future Work

In future, I would like to expand this project to contain almost all controllable home appliances. A smart home automation system will absolutely help people control their home appliances remotely over the internet from anywhere.

ACKNOLODGMENTS

I would like to seize the opportunity to openly give my special thanks to the following people who granted me their support and assistance during my Master's degree course. Dr. Vladimir Dyo for his precious supervision, assistance and comments during the course; Dr.Haider AL-Khateeb for his continuous directions and workshops over the course. My extreme thanks to people who took time completing my questionnaire. I would also like to offer my gratefulness to my family for their full encouragement and support to complete my Master's degree. Finally, my utmost thanks to my best friend for her continuous assistance over the past two years.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Adafruit, (no date), *NPN Bipolar Transistors (PN2222) - 10 pack* [image]. Available at: <https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiph7GQwJ7PAhXlfhoKHSscDAwQjRwIBw&url=https%3A%2F%2Fwww.adafruit.com%2Fproduct%2F756&bvm=bv.133387755,d.d2s&psig=AFQjCNF2Tqfao5l260UJsswEZwpaekoMNQ&ust=14741479981711608> [Accessed 6 September 2016].
2. Al-Ali, A.R. and Al-Rousan, M., 2004. Java-based home automation system. *IEEE Transactions on Consumer Electronics*, 50(2), pp.498-504.
3. AliExpress, (2010), *wholesale ir receiver sensor* [image]. Available at: [https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiCtKPjtZ7PAhWCxxQKHfj\\_CqcQjRwIBw&url=http%3A%2F%2Fwww.aliexpress.com%2F%2Fwholesale-ir-receiver-sensor.html&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNFQSU4yWI7bHpwiD2b6bP1YC1v\\_gg&u=1474477202999505](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiCtKPjtZ7PAhWCxxQKHfj_CqcQjRwIBw&url=http%3A%2F%2Fwww.aliexpress.com%2F%2Fwholesale-ir-receiver-sensor.html&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNFQSU4yWI7bHpwiD2b6bP1YC1v_gg&u=1474477202999505) [Accessed 6 September 2016].
4. Anders, B. 2016. *Windows 10 IoT core support for raspberry pi 3*. [ONLINE] Available at: <https://blogs.windows.com/buildingapps/2016/02/29/windows10-iot-core-support-for-raspberry-pi-3/>. [Accessed 12 April 2016].
5. Azure Austin. (2015). *Windows 10 IoT on Raspberry Pi with Visual Studio and C# Universal Apps*. [Online Video]. 29 November 2015. Available from: <https://www.youtube.com/watch?v=jZpW6EkLZ9U>. [Accessed: 17 May 2016].
6. Baily, S., Paris, J. and Curtis, I. n.d. *WinLIRC*. [ONLINE] Available at: <http://winlirc.sourceforge.net/>. [Accessed 25 May 2016].
7. Bain, A. 2013. *Setting up LIRC on the RaspberryPi - alexba.in*. [ONLINE] Available at: <http://alexba.in/blog/2013/01/06/setting-up-lirc-on-the-raspber-rypi/>. [Accessed 4 September 2016].
8. Bartelmus, C. 2016. *LIRC - Linux infrared remote control*. [ONLINE] Available at: <http://www.lirc.org/>. [Accessed 5 September 2016].
9. Buyapi, (2016), *HDMI TO VGA ADAPTER* [image]. Available at: <https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiE6lipwJ7PAhWLnRoKHZfFAkAQjRwIBw&url=https%3A%2F%2Fwww.buyapi.ca%2Fproduct%2Fhdmi-to-vgaadapter%2F&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNHRqQT7GnYkvXB9xqoloZpKvQGKDg&ust=1474480035052921> [Accessed 6 September 2016].
10. Carretero, J. and García, J.D., 2014. The Internet of Things: connecting the world. *Personal and Ubiquitous Computing*, 18(2), pp.445-447.
11. Celebre, A.M.D., Dubouzet, A.Z.D., Medina, I.B.A., Surposa, A.N.M. and Gustilo, R.C., 2015, December. Home automation using raspberry Pi through Siri enabled mobile devices. In *Humanoid. Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), 2015 International Conference on* (pp. 1-6).IEEE.
12. CES, (2016), *PIR motion sensor module* [image]. Available at: [https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjdl2ytJ7PAhULWRoKHUIMAZAQjRwIBw&url=http%3A%2F%2Fwww.ceseshop.com%2Fdir%2Findex.php%3Froute%3Dproduct%2Fproduct%26product\\_id%3D691&bvm=bv.133387755,d.d2s&psig=AFQjCNEGvpCnTSxFrlwqDnZekl7WmMFHXQ&ust=1474476830366270](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjdl2ytJ7PAhULWRoKHUIMAZAQjRwIBw&url=http%3A%2F%2Fwww.ceseshop.com%2Fdir%2Findex.php%3Froute%3Dproduct%2Fproduct%26product_id%3D691&bvm=bv.133387755,d.d2s&psig=AFQjCNEGvpCnTSxFrlwqDnZekl7WmMFHXQ&ust=1474476830366270) [Accessed 6 September 2016].
13. Circuit Specialists, (2016), *Solder less Breadboards* [image]. Available at: [https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiToDDwJ7PAhUGExoKHftUDhoQjRwIBw&url=https%3A%2F%2Fwww.circuitspecialists.com%2Fsolderlessbreadboards&bvm=bv.133387755,d.d2s&psig=AFQjCNFhZvVC-7Ez-p2-sTww9bYl0FB3\\_g&ust=1474480075353879](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiToDDwJ7PAhUGExoKHftUDhoQjRwIBw&url=https%3A%2F%2Fwww.circuitspecialists.com%2Fsolderlessbreadboards&bvm=bv.133387755,d.d2s&psig=AFQjCNFhZvVC-7Ez-p2-sTww9bYl0FB3_g&ust=1474480075353879) [Accessed 6 September 2016].
14. Gadgetar, (2016), *Raspberry pi 3 model B \$30* [image]. Available at: [https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwillLnVtJ7PAhVHWRQKHRnNB4UQjRwIBw&url=http%3A%2F%2Fwww.gadgetar.com%2Fraspberry-pi-3-modelb%2F&psig=AFQjCNH0c28fbs0\\_m01DowQzmdbYZW95Q&ust=1474476903101223&cad=rjt](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwillLnVtJ7PAhVHWRQKHRnNB4UQjRwIBw&url=http%3A%2F%2Fwww.gadgetar.com%2Fraspberry-pi-3-modelb%2F&psig=AFQjCNH0c28fbs0_m01DowQzmdbYZW95Q&ust=1474476903101223&cad=rjt) [Accessed 6 September 2016].
15. Ganesan, A. 2015. *WARAN - Home Automation*. [ONLINE] Available at: [https://www.hackster.io/arjun/waran-home-automation84a26?ref=challenge&ref\\_id=15&offset=11](https://www.hackster.io/arjun/waran-home-automation84a26?ref=challenge&ref_id=15&offset=11). [Accessed 25 May 2016].
16. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), pp.1645-1660.
17. Harrington, W., 2015. *Learning Raspbian*. Packt Publishing Ltd.
18. IBM. 2016. *SPSS Statistics*. [ONLINE] Available at: <http://www-03.ibm.com/software/products/en/spssstatistics>. [Accessed 9 September 2016].
19. Ivancreations.com. 2016. *Control Air Conditioner with RaspberryPI and a LED*. [ONLINE] Available at: <http://www.ivancreations.com/2015/04/control-air-conditioner-with.html>. [Accessed 3 May 2016].
20. Kopetz, H., 2011. Internet of things. In *Real-time systems* (pp. 307-323).Springer US. Kortuem, G., Kawsar, F., Fitton, D. and Sundramoorthy, V., 2010. Smart objects as building blocks for the internet of things. *Internet Computing, IEEE*, 14(1), pp.44-51.

20. Ma, H.D., 2011. Internet of things: Objectives and scientific challenges. *Journal of Computer science and Technology*, 26(6), pp.919-924.
21. Meetup. 2015. *Building Internet of Things using C#*. [ONLINE] Available at: <http://www.meetup.com/NET-Developers-Association/events/220140826/>. [Accessed 21 May 2016].
22. MODMYPI. 2016. *How to give your Raspberry Pi a Static IP Address - UPDATE*. [ONLINE] Available at: <https://www.modmypi.com/blog/how-to-give-your-raspberry-pi-a-static-ip-address-update>. [Accessed 4 September 2016].
23. Gillett, M. 2015. Low-cost Home Automation with Voice Control. [ONLINE] Available at: [https://www.hackster.io/michael-gillett/dorm-automation-9fed01?ref=challenge&ref\\_id=15&offset=20](https://www.hackster.io/michael-gillett/dorm-automation-9fed01?ref=challenge&ref_id=15&offset=20). [Accessed 25 May 2016].
24. Microsoft. 2016. 'Hello, World!' Sample. [ONLINE] Available at: <https://developer.microsoft.com/enus/windows/iot/win10/samples/helloworld>. [Accessed 14 May 2016].
25. Microsoft. 2016. *Learn about windows 10 IoT core*. [ONLINE] Available at: <https://developer.microsoft.com/en-us/windows/iot/explore/iotcore>. [Accessed 12 April 2016].
26. Microsoft. 2015. *Microsoft Projects*. [ONLINE] Available at: <https://developer.microsoft.com/enus/windows/iot>. [Accessed 12 April 2016].
27. Microsoft. 2016. *The Internet of your things*. [ONLINE] Available at: <https://developer.microsoft.com/enus/windows/iot>. [Accessed 10 April 2016].
28. Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), pp.1497-1516.
29. net-tutorials. 2006. *The complete C# Tutorial*. [ONLINE] Available at: <http://csharp.net-tutorials.com/>. [Accessed 22 May 2016].
30. Microsoft. 2016. *Overview of Visual Studio 2015 Products*. [ONLINE] Available at: <https://www.visualstudio.com/en-us/products/vs-2015-product-editions.aspx>. [Accessed 15 April 2016].
31. raspberrypi.org. 2016. *Build a LAMP Web Server with Word Press*. [ONLINE] Available at: <https://www.raspberrypi.org/learning/lamp-web-server-with-wordpress/worksheet/>. [Accessed 5 September 2016].
32. Rieger, C. 2016. *Raspberry Pi Blind & AC Controller*. [ONLINE] Available at: <http://chrisrieger.com/projects/roomautomation>. [Accessed 24 May 2016].
33. SanDisk , (n.d), *8GB Sandisk MicroSDHC Memory Card with SD Adapter* [image]. Available at: <https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwirocbHtZ7PAhVBnBQKHxNIB5QQjRwIBw&url=https%3A%2F%2Fwww.amazon.com%2FSandisk-MicroSDHC-Memory-Card-Adapter%2Fdp%2FB000WH6H1M&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNGikpcggSgXwgyDN4ZphEhLxO3lyA&ust=1474477100739052> [Accessed 6 September 2016].
34. Sangesari, R. 2015. *Access your Raspberry Pi over the Internet*. [ONLINE] Available at: <https://www.hackster.io/idreams/access-your-raspberry-pi-over-the-internet-157ad1>. [Accessed 9 September 2016].
35. Solarbotics, (n.d), *40 pin Female-to-Female Jumper Cable 45072* [image]. Available at: <https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiXvsjhwJ7PAhXHExoKHeLkDGwQjRwIBw&url=https%3A%2F%2Fsolarbotics.com%2Fproduct%2F45072%2F&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNEm2gdG6H2K0qoqGovHCVtqsQFca&ust=1474480144244078> [Accessed 6 September 2016].
36. Sriskanthan, N., Tan, F. and Karande, A., 2002. Bluetooth based home automation system. *Microprocessors and Microsystems*, 26(6), pp.281-289.
37. Steve Teixeira. 2015. *Hello, Windows 10 IoT Core*. [ONLINE] Available at: <https://blogs.windows.com/buildingapps/2015/08/10/hello-windows-10-iot-core/>. [Accessed 12 April 2016].
38. Tao, F., Zuo, Y., Da Xu, L. and Zhang, L., 2014. IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *Industrial Informatics, IEEE Transactions on*, 10(2), pp.1547-1557.
39. TechshopBD, (2012), *IR Transmitter - White* [image]. Available at: <https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiD9M39tZ7PAhXGXGXRQKHeOzDNQQjRwIBw&url=https%3A%2F%2Fwww.techshopbd.com%2Fproductcategories%2Fflight%2F743%2Ffir-transmitter-white-techshopbangladesh&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNF4vTn5HtAl0ADxrlqpbKsBQEL9MQ&ust=1474477258911023> [Accessed 6 September 2016].
40. Vasanwala, A.S. 2015. Home Automation using Raspberry Pi 2 and Windows 10 IoT. [ONLINE] Available at: [https://www.hackster.io/AnuragVasanwala/home-automation0dcefc?ref=challenge&ref\\_id=15&offset=2](https://www.hackster.io/AnuragVasanwala/home-automation0dcefc?ref=challenge&ref_id=15&offset=2). [Accessed 25 May 2016].
41. Vis, P.J., (n.d), *10k / 10k ohm Resistor Colour Code* [image]. Available at: [https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwiVh\\_bTvZ7PAhXBixKHUcDcEwQjRwIBw&url=http%3A%2F%2Fwww.petervis.com%2Felectronics%2Fstandard\\_Resistor\\_Values%2F10K.html&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNHwYc-WVntd\\_DyEVBHB8z7TNG7w&ust=1474479311654384&cad=rjt](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwiVh_bTvZ7PAhXBixKHUcDcEwQjRwIBw&url=http%3A%2F%2Fwww.petervis.com%2Felectronics%2Fstandard_Resistor_Values%2F10K.html&bvm=bv.133387755,bs.2,d.d2s&psig=AFQjCNHwYc-WVntd_DyEVBHB8z7TNG7w&ust=1474479311654384&cad=rjt) [Accessed 6 September 2016].
42. WiringPi. 2016. *WiringPi*. [ONLINE] Available at: <http://wiringpi.com/>. [Accessed 4 September 2016].

Wortmann, F. and Flüchter, K., 2015. Internet of Things.

41. Xia, F., Yang, L.T., Wang, L. and Vinel, A., 2012. Internet of things. *International Journal of Communication Systems*, 25(9), p.1101.

42. Zhu, J., Gao, X., Yang, Y., Li, H., Ai, Z. and Cui, X., 2010, September. Developing a voice control system for zigbee-based home automation networks. In *2010 2nd IEEE International Conference on Network Infrastructure and Digital Content* (pp. 737-741). IEEE.

## APPENDIX A: USER SATISFACTION QUESTIONNAIRE

### User Satisfaction Questionnaire

Dear SANYO split air conditioner users; Smart Air Conditioner Using Internet of Things Product helps you to remotely control your air conditioner through a web application from any windows physical device such as a desktop, a laptop, a PAD and a smart phone you possess. The implemented smart air conditioner would be able to turn off by itself when people are not present and save energy. Results of the survey will be treated with full confidentiality and it will be stored in a secure place. Likewise, the obtained results will be used to monitoring your satisfaction as a customer and to identifying improvements to the product.

I am looking forward to your cooperation to conduct the questionnaire.

Gender:

Male

Female

Age: .....

1. I am interested on home automation services.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

2. The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

3. The system is easy to use.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

4. I feel much more comfortable to use this system than the local remote control.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

5. I recommend using this system as a product in technology market.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

Thank you for your valuable time...



## APPENDIX B: IMPLEMENTATION SOURCE CODE

## Section I: PIR Sensor Source Code:

```

import time
import os
import RPi.GPIO as gpio
pir = 4 // define PIN 4 in Raspberry Pi 3 GPIO as a variable called pir
gpio.setmode(gpio.BCM)
gpio.setup(pir, gpio.IN) // define PIN 4 in Raspberry Pi 3 GPIO as an INPUT PIN
n = 0
while True: // While loop
ir = gpio.input(pir)
print ir
if ir == 0: // when output from PIR Sensor is LOW
n = n+1
time.sleep(1) // set the time delay equals to 1 second
if n > 1800:
n = 2000
else:
n = 0
time.sleep(1) // set the time delay equals to 1 second
/* if PIR Sensor does not sense any presence or motion, it will ask Raspberry Pi 3 to turn off the ac
automatically */
if n == 1800:
os.system("irsend SEND_ONCE ir1.conf KEY_POWER2")
time.sleep(10)

```

Section II: *iotAC.php* Source Code:

```

<html>
<head>
<meta name="viewport" content="width=device-width" />
<title>AC Control</title> // set the name of the web page to AC Control
</head>
<body>
<?php
echo "<body style='background-color: PowderBlue'>"; // set the background color of the web page
echo'
<html>
/* Insert image into the web page */

</html>
';
?>

 // create a break = line space
AC Remote Control:

 <form method="get" action="iotAC.php">
<input type="submit" value="ON" name="on" style="width: 50px; height: 50px;">
<input type="submit" value="OFF" name="off" style="width: 50px; height: 50px;">

<input type="submit" value="+" name="p" style="width: 50px; height: 50px;">
<input type="submit" value="-" name="n" style="width: 50px; height: 50px;">
</form>
<?php
/* If user click on ON button, Raspberry Pi will execute a shell command to turn on the AC */
if(isset($_GET['on'])){
$gpio_on = shell_exec("irsend SEND_ONCE ir1.conf KEY_POWER");

```



```

echo "AC is on"; // display 'AC is on' message
}
/* If user click on OFF button, Raspberry Pi will execute a shell command to turn off the AC */
else if(isset($_GET['off'])){
$gpio_off = shell_exec("irsend SEND_ONCE ir1.conf KEY_POWER2");
echo "AC is off"; // display 'AC is off' message
}
/* If user click on + button, Raspberry Pi will execute a shell command to increase temperature volume of
the AC */
else if(isset($_GET['p'])){
$gpio_p = shell_exec("irsend SEND_ONCE ir1.conf KEY_UP");
echo "Temperature is increased"; // display 'Temperature is increased' message
}
/* If user click on - button, Raspberry Pi will execute a shell command to decrease temperature volume of
the AC */
else if(isset($_GET['n'])){
$gpio_n = shell_exec("irsend SEND_ONCE ir1.conf KEY_DOWN");
echo "Temperature is decreased"; // display 'Temperature is decreased' message
}
?>
</body>
</html>

```

Section II: login.php Source Code:

```

<html>
<head>
<meta name="viewport" content="width=device-width" />
<title>AC Control</title> // set the name of the web page to AC Control
</head>
<body>
<div align="center"> // make content of the web page in the center
<?php
echo "<body style='background-color:PowderBlue'>"; // set the background color of the web page
?>
<form id='login' action='submit.php' method='post' accept-charset='UTF-8'>
<fieldset >
<legend>Login</legend>
<input type='hidden' name='submitted' id='submitted' value='1'/>
<label for='username' >UserName</label> // create a button on the web page named UserName
/* specify the type of UserName button is a text and set the length of the entered username equals to 100
*/
<input type='text' name='username' id='username' maxlength="100" />
<label for='password' >Password</label> // create a button on the web page named Password
/* specify the type of Password button is a text and set the length of the entered password equals to 100 */
<input type='password' name='password' id='password' maxlength="100" />
/* create a button on the web page named Submit and specify the type of it as submit */
<input type='submit' name='Submit' value='Submit' />
</fieldset>
</form>
</body>
</html>

```

Section IV: submit.php Source Code:

```

<html>
<head>
<meta name="viewport" content="width=device-width" />
<title>AC Control</title> // set the name of the web page to AC Control
</head>

```

```

<body>
<div align="center">
<?php
echo "<body style='background-color:PowderBlue'>"; // set the background color of the web page
session_start();
/* Declare Variables */
$field1 = $_POST['username']; // this is the username variable posted from login.php web page
$field2 = $_POST['password']; // this is the password variable posted from login.php web page
/* If the user missed enter the username and password in login.php page */
if (($POST['username'] == "") || ($POST['password'] == "")){
/* display sorry.. There are some missing required information message */
echo"sorry.. There are some missing required information ";
include("login.php"); // direct the user to login.php web page
echo'
'; // create a break = line space
echo'
';
echo'
';
die(mysql_error());
exit;
}
include("header.php"); // refer to header.php web page for required information to connect to MySQL
server
/* connect to MySQL server using host, username and password declared in header.php */
mysql_connect($host,$username,$password);
/* select the database declared in header.php */
mysql_select_db($database);
/* query the database to select all records in login table in ac_control database */
$query= "SELECT * FROM login";
/* save data received from performing the above query in a variable called result */
$result=mysql_query($query);
/* If the query failed to perform the action */
if (!$result) {
/* display 'Could not run query: 'message and exit MySQL Server */
echo 'Could not run query: ' . mysql_error();
exit;
}
/* declare a variable called num that saves the number of rows in login table */
$num=mysql_numrows($result);
$i=0;
// While loop: as long as the variable i is less that the number of rows in login table, fetch the row of the table and
check if row[0] which is username in login table equals to the username posted from login.php and row[1] which is
password in login table equals the password posted from login.php, direct the user to iotAC.php web page. If not,
display 'error' message */
while($i < $num){
$row= mysql_fetch_row($result);
if (($row[0]==$field1) && ($row[1]==$field2))
{
include("iotAC.php");
}
else
{
echo 'error';
}
$i++;
}
?>

```

Section V: header.php Source Code:

```
<?php
/* set the 'root' username used to access MySQL Server in a variable called username */
$username="root";
/* set 'mysql' password used to access MySQL Server in a variable called password */
$password="mysql";
/* set ac_control database in a variable called database */
$databse="ac_control";
/* set localhost (the location where the database is stored) in a variable called host */
$host="localhost";
?>
```

APPENDIX C:

Smart Air Conditioner using Internet of Things Poster

**Background** Internet of Things (IoT); an emerging technology has risen in the digital realm. The original idea of Internet of Things was proposed at the end of 1990's. IoT is much more related to the wireless sensors networks, mobile communications networks and internet. IoT can be defined as a network that connects every existing physical object in the world to a unique address in order to provide quick and smart services. Hence, with Internet of Things, you may control everything using internet service.

**Problem** As it is known, the usual and traditional mechanism in which the end user controls the air conditioner is through local remote control.  
 •However, what if the local remote control is lost, broken, out of batteries or no longer available due to whatever faulty?  
 •On the other hand, what if the air conditioner is forgotten on due to human nature and no one is available to turn it off?  
 •How about controlling the temperature degree of your air conditioner while you are actually away?  
 •How about having a smart air conditioner that would be able to turn off by itself when people are not present and save energy?  
 •Reaching this point, Automation feature seems the best logical solution to handle and control the air conditioner remotely.

**Aim** The aim of this project is to design and implement a smart air conditioner using Internet of Things technology using Raspberry Pi 3 Model B device.

**Objectives**

- Review related home automation system literatures.
- Select the most suitable platform (Raspbian: the most popular platform used with Raspberry Pi or Windows 10 IoT core: the new platform developed by Microsoft) to design and implement the smart air conditioner.
- Test, validate and explore the gained features of the product.

**Results**

**Evaluation**

The obtained statistics from analyzing the questionnaire, the implemented smart air conditioner product is obviously gaining trust of the potential users. This is the statistics of one of five questions:

The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.

|                |         |                     |
|----------------|---------|---------------------|
| <b>N</b>       | Valid   | 14                  |
|                | Missing | 0                   |
| <b>Mean</b>    |         | 4.5714              |
| <b>Median</b>  |         | 4.5714 <sup>a</sup> |
| <b>Maximum</b> |         | 5.00                |

The system helped me to control my air conditioner unit remotely from anywhere using any device with a web browser.



# Trust-Based Security Technique to Curb Cooperative Blackhole Attacks in Mobile Ad Hoc Networks using OTB-DSR Protocol in NS-3

By Ephantus Gichuki Mwangi, Geoffrey Muchiri Muketha  
& Gabriel Ndung'u Kamau

*Murang'a University of Technology*

**Abstract-** The advent of mobile technology led to the emergence of Mobile Ad-hoc networks (MANETs). These networks have no infrastructure and central authority. Nodes in MANETs act as both routers and hosts. MANET nodes join and leave the network at will making the network topology dynamic. MANETs are prone to both passive and active security attacks. Blackhole is a denial of service attack under active attacks. Blackhole nodes work in collaboration forming cooperative black hole attacks. The attacks drop or redirecting data packets on transit. Cooperative blackhole attacks are dangerous in operations where communication is critical. This paper proposes a Trust-Based Resilient Cooperative Bait Detection Technique (TB-RCBDT), an integration of the Resilient Cooperative Bait Detection Technique (RCBDT) and Optimized Trust-Based Dynamic Source Routing (OTB-DSR).

**Keywords:** routing protocol, mobile ad hoc network, security.

**GJCST-E Classification:** C.2.0



TRUSTBASESECURITYTECHNIQUETOCCURBLACKHOLEATTACKSINMOBILEADHOCNETWORKSUSINGOTBDSRPROTOCOLINNS3

*Strictly as per the compliance and regulations of:*



RESEARCH | DIVERSITY | ETHICS



# Trust-Based Security Technique to Curb Cooperative Blackhole Attacks in Mobile Ad Hoc Networks using OTB-DSR Protocol in NS-3

Ephantus Gichuki Mwangi <sup>α</sup>, Geoffrey Muchiri Muketha <sup>σ</sup> & Gabriel Ndung'u Kamau <sup>ρ</sup>

**Abstract-** The advent of mobile technology led to the emergence of Mobile Ad-hoc networks (MANETs). These networks have no infrastructure and central authority. Nodes in MANETs act as both routers and hosts. MANET nodes join and leave the network at will making the network topology dynamic. MANETs are prone to both passive and active security attacks. Blackhole is a denial of service attack under active attacks. Blackhole nodes work in collaboration forming cooperative black hole attacks. The attacks drop or redirecting data packets on transit. Cooperative blackhole attacks are dangerous in operations where communication is critical. This paper proposes a Trust-Based Resilient Cooperative Bait Detection Technique (TB-RCBDT), an integration of the Resilient Cooperative Bait Detection Technique (RCBDT) and Optimized Trust-Based Dynamic Source Routing (OTB-DSR). The proposed technique aims at mitigating collaborative black hole attacks. Design, implementation, and simulation of the TB-RCBDT technique was done in Network Simulator Version 3 (NS-3). TB-RCBDT technique was compared to Cooperative Bait Detection Scheme (CBDS) and Extended Cooperative Bait Detection Scheme (ECBDS) used as benchmark schemes. Simulation results show that the proposed technique is superior to benchmark techniques. Metrics used to evaluate the performance of the proposed technique were packet delivery ratio, end-to-end Delay, routing overheads, and energy consumption.

**Keywords:** routing protocol, mobile ad hoc network, security.

## 1. INTRODUCTION

MANETs are wireless, with no infrastructure, and central management authority. These networks are dynamic nodes join and leave the network at will. MANETs work in areas where wired networks fail either due to destruction or natural catastrophes such as earthquakes, storms, eruptions, or terrorism [1], [2].

In MANETs, nodes communicate through special routing protocols [1], [2]. Researchers have developed several routing protocols and techniques to optimize MANETs' security [2], [6]. However, design issues are surrounding MANETs routing protocols and techniques. Some of the issues are related to the unique properties of MANETs. These issues make most of the security

techniques designed for wired networks incompatible with MANETs [3].

MANETs routing protocols are grouped into three categories. The categories include; reactive routing protocols, proactive routing protocols, and hybrid protocols. Reactive routing protocols are demand-driven. They create routes whenever a source node wishes to send data packets to a destination node. This implies that nodes that actively participate in routes formation are the ones that maintain valid routing information. Some of the examples of reactive routing protocols are Adhoc On-Demand Vector (AODV), Dynamic Source Routing (DSR), and Link Aware Routing (LAR) [6]. In proactive protocols, nodes maintain complete routing information of the network. Any change of network topology due to nodes' mobility leads to automatic updating of routing tables. Some of the examples of proactive routing protocols are; Destination Sequenced Distance Vector (DSDV), Global State Routing (GSR), and Hierarchically Segmented Routing (HSR) protocols. Hybrid protocols contain blended features of both proactive and reactive routing protocols [4].

The open form of communication in MANETs paves way for an attacker to join and intercept the communication process. Further, the unique properties of MANETs have introduced an underlying complex security problem [5], [7]. Cooperation amongst nodes has made MANETs vulnerable to many network security threats. Therefore, in the design of effective security techniques secure transmission should be a key consideration [5], [7], [25].

Blackhole attack is one of the popular active attacks that endanger network integrity. Blackhole nodes drop data packets between any two communicating nodes that establish a connection [7]. For instance, a source node can send Route Request (RREQ) packets to establish a communication with the destination node. Any node in the network that has the shortest route to the destination can respond to the RREQ packet. This open form of communication paves the way for blackhole nodes to join in the communication process. For instance, when the black hole nodes receive the RREQ packet, they masquerade as genuine nodes by sending fake RREP packets with the shortest and freshest route to the destination. This

**Author  $\alpha$   $\rho$ :** Department of Information Technology, Murang'a University of Technology, 75-10200, Murang'a, Kenya.

**Author  $\sigma$ :** Department of Computer Science, Murang'a University of Technology, 75-10200, Murang'a, Kenya.  
e-mail: egmkuc@gmail.com

makes the source node to select the route with malicious nodes. However, when these black hole nodes receive the data packets they drop or reroute them to fake destinations. Further, black hole nodes collaborate to launch attacks known as 'cooperative black hole attacks'. The cooperative black hole attacks are more harmful to a network than any other form of attack [8], [20].

Techniques such as CBDS and ECBDS suffer from security and performance issues. These issues are attributed to packet delivery ratio (PDR), end to end delays, and routing overhead. Most of the security issues arise from architecture and design considerations of the techniques. For instance, in CBDS and ECBDS techniques a source node takes some time to identify and use bait address from one of its immediate neighbours. This contributes to end to end delays. Further, these techniques do not have an effective mechanism of identifying genuine nodes in the network which leads to the incorporation of blackhole nodes in the transmission process. Additionally, genuine nodes transmit data packets without checking their energy levels. This opens an opportunity for the depleted nodes to transmit; hence acting selfishly. Selfish nodes drop data packets to save energy for their sustenance.

The study proposes a TB-RCBDT technique using the OTB-DSR protocol to identify and mitigate collaborative black hole attacks. TB-RCBDT used Resilient Cooperative Bait Detection Technique (RCBDT) which uses source node self-address as the bait address. Source node self-address saves transmission bandwidth, node's energy, and time. Further, RCBDT uses an algorithm that checks energy levels for all genuine nodes before engaging them in any transmission. In case there are nodes whose energy levels are below the threshold, it gives alerts to the source node. Additionally, TB-RCBDT uses the trust concept through the OTB-DSR protocol to identify malicious nodes in the network.

The design, implementation, and simulation of TB-RCBDT were done in a Linux environment using NS-3. Further, the technique was tested alongside CBDS and ECBDS used as benchmark techniques.

The rest of the paper is organized as follows; Section 2 presents related works, section 3 is a discussion of the methodology used. Section 4 describes the simulation environment. Further, section 5 presents the results and discussions. Finally, section 6 summarizes the study by giving conclusions and future work.

## II. RELATED WORK

Abdelshafy and King proposed a mechanism (BRM) using the AODV protocol [6]. Its purpose was to mitigate the black hole attack. Simulation results showed that BRM-AODV was superior to AODV and

SAODV routing protocols in all network performance metrics. BRM detected black hole nodes easily regardless of their number. Additionally, results showed that BRM increased the performance of AODV routing algorithms in MANETs. However, BRM-AODV failed to detect collaborative black hole attacks. Reviewed literature indicates that no enhancement of the BRM has been done.

Ukey proposed a 1-2ACK technique to curb routing attacks in MANETs [16]. 1-2ACK creates sets of three adjacent nodes for all the nodes that form routes for transmitting packets. This technique detected and mitigated black holes' attacks. However, the technique introduced extra control packets which led to routing overheads.

Hiremani and Jadhao developed a security technique using modified extended data routing information (MEDRI) using the routing table of the AODV protocol [17]. The technique was capable of detecting cooperative black hole attacks. MEDRI table maintained a record of the history of the previous malicious nodes. This record was used for the future discovery of secure paths from source to destination. However, the technique suffered from routing overhead and end to end delay.

Mistry et al. proposed a security technique that uses the source node to receive the first RREP [9]. Further, the technique waits for a specified time interval before receiving and storing the other RREPs. The source node analyses all the RREPs and rejects the ones with a very high sequence number. However, simulation results indicate that the technique increased average end to end delay.

Su et al. proposed a technique using an intrusion detection system (IDS) [10]. The purpose of IDS nodes is to detect the malicious value of nodes based on the difference between RREQs and RREPs forwarded by a node. However, if the malicious value goes beyond the threshold, the node is considered malicious. This makes the IDS node broadcasts a block message to all nodes on the network. The technique introduced extra nodes in the network. Further, IDS sniffed all the RREQs and RREPs of all nodes that led to extra overhead.

Gupta et al. proposed a technique using Ad hoc On-Demand Multipath Distance Vector (OMDV) [11]. The technique provided multiple paths during routes establishment. The source node selects only one route among available ones. The node maintains the legitimacy of all its neighbouring nodes. The technique ensures that the route selected does not include nodes with legitimacy value less than the threshold. This helps in detecting and avoiding malicious nodes. However, the technique was not able to detect cooperative blackhole nodes.

Saha et al. proposed a Two-Level Secure Routing (TSR) [12]. The technique uses Local

Supervision (LS) and Congestion Window Surveillance (CWS) modules to detect malicious attacks. TSR addresses these attacks using the Alternate Route Finder (ARF) module. ARF module does the work of re-routing packets at the network layer. Simulation results showed that the proposed technique is resilient against various attacks. However, LS and CWS modules introduced routing overhead.

Bhosle proposed a watchdog and pathrater mechanism [13]. The technique ensures that each node maintains a pending packet table and node rating table. Each node stores all packets forwarded in the pending packet table and overhears its neighbours. If the neighbouring node successfully forwards the packet, the value of the packet forwarded in the node rating table is incremented. However, if the packet is dropped, the value is decremented. Additionally, if the value of dropped packets gets to the threshold value, that node termed as malicious. This used extra memory space to maintain extra tables which translated to routing overhead.

Thachil presented a technique that does the overhearing of neighbouring nodes to calculate their trust value [14]. Before a node forwards the packet, it keeps a copy in the cache. Additionally, a node overhears the packets forwarded by its neighbours. If a packet forwarded by the neighbour matches with the packet in the cache, the sending node believes that the neighbouring node is genuine. However, if the packet doesn't match the trust value is decremented. If the trust value goes beyond the threshold, that node is considered malicious. The technique introduced routing overhead at a node.

Bindra et al. developed a security technique that uses the AODV protocol [15]. The proposed technique keeps an extended data routing information (EDRI) table in every node. This technique discovers secure paths by avoiding cooperative black hole nodes. However, the challenge of this technique is that malicious nodes must be contiguous to be discovered. Further, the introduction of the EDRI table led to routing overhead.

Gaikwad and Ragha developed a cooperative cluster agents (CCAs) technique to mitigate cooperative black hole attacks [18]. The technique uses DRI and SRT-RRT tables as input to CCAs. Simulation results showed that the technique detected cooperative black hole nodes. Additionally, the technique identified a secure routing path from source to destination. This technique was compared to the standard AODV protocol. Results show that the technique proved to be superior. However, CCAs technique introduced routing overhead due to the incorporation of DRI and SRT-RRT tables. Further, packet delivery ratio and throughput need further improvement to hit the desired levels.

Dumne and Manjaramkar proposed a Cooperative Bait Detection Scheme (CBDS) based upon

the DSR mechanism [19]. The scheme integrates proactive and reactive defence architectures to detect malevolent nodes. Simulation results showed that CBDS using AODV was superior to DSR protocol and CBDS using DSR. Metrics used in this scheme were throughput and packet delivery ratio. However, the proposed technique was inferior to CBDS using AODV in terms of throughput and packet delivery ratio. This is a motivation for researchers to enhance the new technique. Further, the reverse tracing technique led to the end to end delay in data transmission.

Emimajuliet and Thirilogasundari proposed Modified Cooperative Bait Detection Scheme (MCBDS) based on DSDV [20]. MCBDS is a modification of CBDS. Simulation results showed that MCBDS with DSDV protocol was superior to DSR and 2ACK scheme. However, MCBDS suffered from routing overhead. Reviewed literature shows that there is a need for a hybrid technique that can combine MCBDS with other techniques to provide a resilient technique that can secure routing of data packets.

Mwangi, Meath, and Kamau proposed a Resilient Cooperative Bait Detection Technique (RCBDT) using DSR protocol in NS3 to curb collaborative black hole attacks [29]. The proposed technique used the source node address as the bait address. Further, the RCBDT used an algorithm that checks nodes' energy levels before engaging them in packet transmission. The proposed technique was compared with CBDS and ECBDS used as benchmark techniques. Simulation results indicated that the proposed technique was superior to benchmark techniques. Metrics used were packet delivery ratio, end-to-end delays, and routing overheads. The findings showed that RCBDT had the highest packet delivery Ratio of 94%, while ECBDS and CBDS had 88% and 81% respectively. Additionally, simulation results indicated that RCBDT had the lowest routing overhead of below 8% while ECBDS and CBDS had 15% and 19% respectively. Finally, results indicated that RCBDT had an end-to-end delay of 1.2 seconds while ECBDS and CBDS which had an average of 1.3 and 1.8 seconds.

Mwangi, Meath, and Kamau proposed an Optimized Trust-Based Dynamic Source Routing (OTB-DSR) protocol in NS3 [30]. The proposed protocol integrates dynamic trust and friendship functions in the architecture of standard DSR protocol. The performance of the OTB-DSR protocol was compared to standard DSR and AODV used as the benchmark protocols. Simulation results indicated that the proposed protocol was superior to standard DSR and AODV protocols used as the benchmark protocols. Performance metrics used include; packet delivery ratio, routing overhead, end to end delays, and throughput used as performance metrics. The OTB-DSR protocol had a packet delivery ratio of above 95%, routing overhead of

4.75%, an end to end delay of between 0.9 seconds and 1.65 seconds, and throughput of 95.6 Kbps.

### III. METHODOLOGY

The architecture of the proposed technique was first designed. In the next section, the architecture was translated into a flowchart. Further, in the next section, a detailed description of the proposed technique was provided. In the next section, a demonstration of how the proposed technique computes trust weights in source routes was done. In the next section algorithms of the proposed technique and SROC were developed. Further, in the next section, the technique was implemented in NS-3 programming language. The next

section was a discussion of the results of the proposed technique. Finally, the last section was the conclusion and future work.

#### a) The Architecture of TB-RCBDT Technique

The architecture is made up of integration of RCBDT and OTB-DSR. The two components interact to identify safe and resilient routes as shown in Figure 1. Further, besides the architecture combining the merits of both proactive and reactive defines architectures. It also employs the concept of trust values and energy levels of a node when selecting optimal routes from the node's cache. These factors make the selected source route stand higher chances of being free from malicious attacks during the data transmission process.

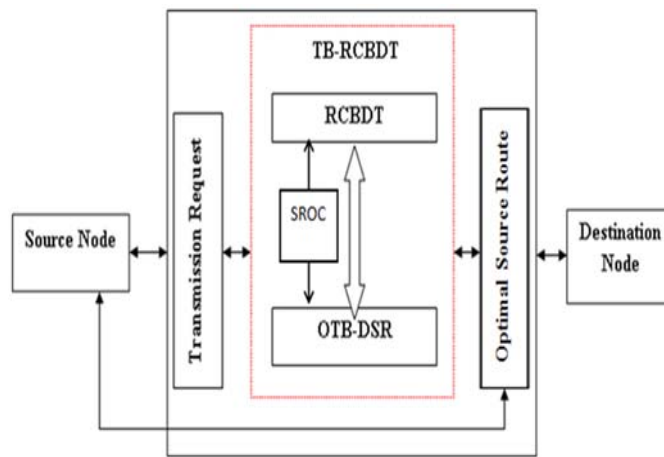


Figure 1: TB-RCBDT Architecture

#### b) Source Route Optimization Component (SROC)

The primary purpose of this component is to select the most optimal route among the prioritized routes. The selected route is marked as the backbone route for packets transmission. The other routes in the node cache are marked as secondary routes. However, in case the selected route turns out to be invalid or

broken, the route refresher component in liaison with the OTB-DSR protocol refreshes the source routes. The information about the fresh source routes is circulated to all the nodes in the network so that they can update their nodes' caches. The block diagram in Figure 2 is a diagrammatic representation of the SROC module.

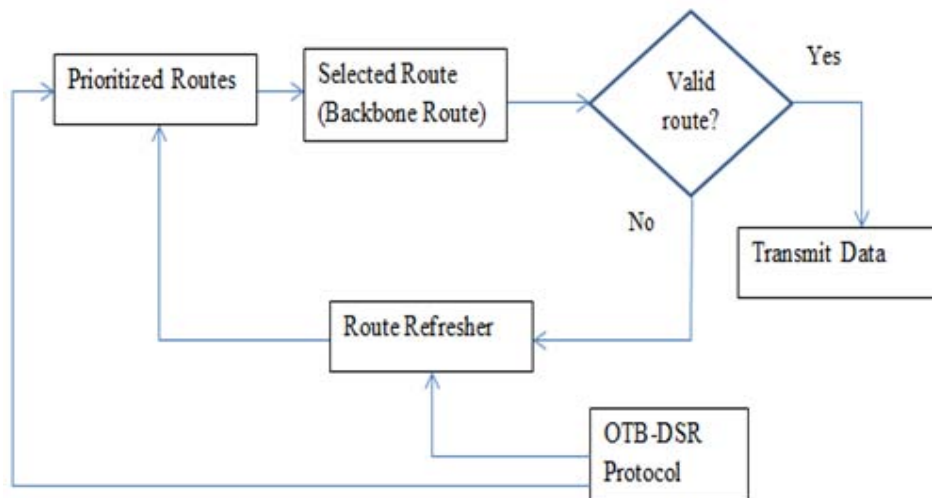


Figure 2: Block Diagram of SROC



c) *Flowchart of TB-RCBDT Technique*

The flowchart of the TB-RCBDT technique is shown in Figure 3. The technique comprises of integration between Optimized Trust-Based DSR protocol and RCBDT design. The primary purpose of RCBDT is to bait all the malicious nodes in the network. Further, RCBDT is also responsible for determining the energy level for all nodes to establish genuine nodes in the network. Any node with an energy level far above the expected level is considered to be malicious; hence blacklisted. Genuine nodes with energy levels above the threshold level and within the limits of acceptable nodes' energy levels are engaged in packet transmission.

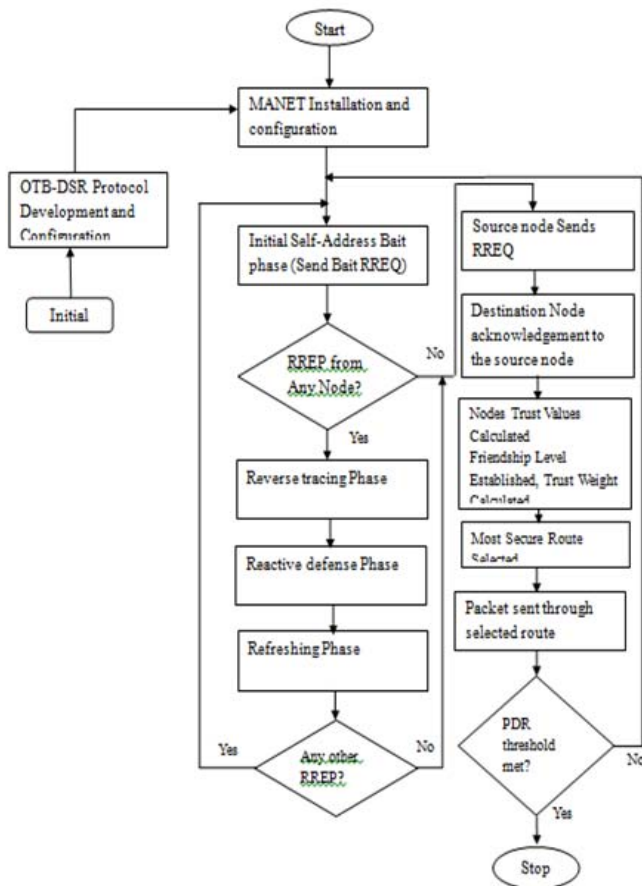


Figure 3: TB-RCBDT Flowchart

d) *Description of Proposed TB-RCBDT Technique*

Trust-Base Resilient Cooperative Bait Detection technique comprises two major components namely; 1) RCBDT, and 2) OTB-DSR. TB-RCBDT technique sets its threshold Packet Delivery Ratio to 97%, routing overhead to below 10%, and end-to-end delays to below 2 seconds. The proposed technique has four phases which include; initial self-address bait phase, reverse tracing phase, reactive defence phase, and refreshing phase.

e) *Initial Self-Address Bait phase*

The phase uses the address of the source node (self-address) as the bait address. This is opposed to

the initial bait phase of CBDS and ECBDS which randomly chooses the address of one of its nearest hop neighbours as its bait destination address. The source node sends bait RREQ with its address as the destination address and waits for a reply from other nodes in the network. OTB-DSR protocol helps in broadcasting this self-address to all its neighbours through the flooding process. A 'Flooding Controller' is used which reduces the lifetime of RREQ packets by every hop. FC will ensure that the flooded RREQ packets automatically eliminate themselves in the network. This will lead to efficient utilization of the bandwidth and also control routing overhead. Further, the TV will help in identifying the most reliable backbone nodes as their selection will be based on the value stored in the TV packet.

Any node that sends the RREP packet is considered a malicious node in the network. The malicious nodes are the fake nodes that receive the route request packet and masquerade to be genuine nodes by sending fake RREP packets with the highest frequency. This triggers the reverse tracing program as indicated in the next phase.

Using self-address as the bait address makes the source node to save its battery power. This power could have been used when communicating with one hop step neighbour to generate the bait address. Further, this also saves time and other network resources as no engagements are involved between the source node and its one-hop step neighbours, hence improving network efficiency.

f) *Reverse Tracing Phase*

In this phase, the reverse tracing program is started to detect the routes with malicious nodes. If the routes are secure, no node send san RREP packet since the source node had broadcasted its address. When malicious nodes receive RREQ, they respond to false RREPs. This triggers the reverse tracing program which tries to identify the dubious paths and exact location of the malicious nodes through the RREPs.

The reverse tracing program then forms a set (Nd) of all the nodes that sent back the false RREPs and saves them in the malicious nodes alarmed list. The source node uses this set (Nd) to form a malicious node detected list. It then sends an alarm to all other nodes in the network about the existence of the malicious nodes. The malicious nodes detected list helps other nodes to establish temporary a set of trusted routes in the network.

$$Nd = \{n_1, n_2, n_3, \dots, n_m\} \quad (1)$$

This phase saves a lot of node's battery power and memory space as no set difference operation is computed to identify the malicious nodes. In ECBDS, when the node received RREP, it would perform a set difference operation between the address List recorded



in RREP and saved RREQ. Further, it would cache the routing of receiving nodes and consequently obtain a new list of genuine nodes. This process drained battery power and memory space, hence limiting its ability to participate in subsequent data transmission processes.

g) *Reactive Defence Phase*

In this phase, first, the reverse tracing program is terminated. Additionally, all the nodes in the malicious node detected list (blackhole list) are deactivated by setting their life-bit bit to zero (sleep mode). Further, this information is broadcasted to all other nodes in the network. Secondly, the OTB-DSR route discovery phase gets triggered. OTB-DSR ensures that Cumulative Trust Values (CTV) and Friendship Level (FL) of every node in the network are computed before the node is engaged. The route discovery process introduces a set of special nodes known as backbone nodes which helps in the fast selection of new routes. The selection of these backbone nodes is based on factors such as; nodes' availability, nodes' signal strength, nodes' cumulative trust value, nodes' friendship level, and energy levels of nodes. The CTV and FL help in identifying reliable primary routes and backbone nodes.

The backbone address challenges of link breakages due to failure or node unreachability. These backbone nodes are reliable neighbouring nodes on standby. Further, they are closer to the optimal routing path nodes and have good signal strength and sufficient power. This improves the efficiency of the technique by guaranteeing the transmission of data packets without any transmission issues. When some of the reliable intermediary nodes get out of range a link failure can occur. In such a case, backbone nodes take charge of the process and the route is re-established without delay. The backbone nodes are selected at one hop distance from the affected node using the gratuitous technique.

h) *Refreshing Phase*

In this phase, the nodes' route caches are refreshed. Broken links are deleted and newly established temporary trusted routes are saved in the nodes caches. Further, the newly recorded routes in the cache are used to determine the optimal route based on the current status of the network. These routes remain valid as long as there are no broken links or no gratuitous routes established. Additionally, the life-bit of nodes classified as genuine is incremented by one, and information circulated to all other nodes in the network. These nodes are allowed to participate in network operations as long as their battery power is above the threshold level.

i) *Computation of Trust Weights in Source Routes*

TB-RCBDT technique uses the OTB-DSR protocol to calculate the nodes' trust values (TV) and friendship level (FL). The two parameters create an array

of source routes weights 'S<sub>naw</sub>' which are saved in the node's cache. Equation 6.1 is an array of calculated source routes weights stored in node X's cache. From equation 6.1, 'w' is the weight of the route while 'α' is a variable representing the dynamic variation of trust in nodes of a given route based state and time.

The weight of a route can be any integer value based on the node's social group level and trust recommendations (RTV) made by neighbouring nodes based on positive or negative interactions during packet forwarding. Equation 6.2 shows how to calculate the weights of every source route. From equation 6.2, 'λ' is a moderating constant. This constant maps the aggregated trust weight of a source route between 0 and 1. Value '0' represents the absence of trust while value '1' represents total trust. The trust weights of routes are spread out between the two values. Source routes with most of the nodes from Most Trusted Friendship Level are the most secure routes since their route trust values are close to '1'. However, if source routes have most of the nodes from Untrusted Friends Level, they are the least secure routes since their route trust values are close to '0'.

$$R_s [] = \{S_{1\alpha w}, S_{2\alpha w}, S_{3\alpha w}, S_{4\alpha w}, \dots, S_{5\alpha w} \} \quad (2)$$

$$W_{n=(RTV_{sn} * \sum_{i=1}^n FL)} * \lambda \quad (3)$$

The Route Selector module prioritizes the source routes based on the aggregated weights. Source routes with aggregated trust weights greater than 0.5 or equal to 1 (0.5 = <W<sub>n</sub> <= 1) are considered to be more trusted. Further, source routes with aggregated trust weights less than 0.5 (0 = <W<sub>n</sub> < 0.5) are considered untrusted.

The proposed TB-RCBDT technique evaluates the received packets at the destination node. Further, it determines whether they meet the packet delivery ratio threshold. If the PDR is below the threshold level, the technique triggers the destination node making it to send a Negative Acknowledgement (NACK) packet to the source node. Further, the source node redirects control to the Bait Phase where a fresh retransmission process is initiated. However, if the PDR is within the threshold level, the proposed technique triggers the destination node making it to send a Positive Acknowledgement (ACK) packet to the source node. The presence of the ACK packet at the source node end means that the handshake process was successful.

j) *Algorithm of TB-RCBDT Technique*

The TB-RCBDT algorithm describes in non-technical terms a step by step process of the implementation of the technique. Further, the algorithm describes all the steps and processes undertaken by a node willing to send packets to the destination. Any node wishing to send data packets triggers the RCBDT algorithm which sends bait RREQ packet over the

network. The purpose of the bait RREQ packet is to detect any malicious node in the MANET.

Response to bait RREQ packet indicates the presence of malicious nodes in the network. This makes the RCBDT algorithm to mark them as malicious, blacklist, and deactivate them. Further, the algorithm identifies the genuine nodes, increases their life bit. Finally, the algorithm calculates their energy levels. The algorithm triggers the source node to send RREQ which identifies a safe route to channel the data packets. When the RREQ reaches the destination node, this node sends back an RREP packet to acknowledge the receipt of the RREQ packet sent by the source node.

The OTB-DSR protocol calculates the composite trust values of all the intermediate nodes that successfully passed the RREQ packet. These composite trust values are stored in the node caches.

Further, the OTB-DSR protocol uses the composite trust values to calculate the friendship level of all the nodes. Finally, the OTB-DSR protocol uses the nodes' composite trust values and friendship level to calculate the route trust weights.

Further, the TB-RCBDT technique uses the SROC module to select the route with the highest Route Trust Value. This route is marked as the backbone route. The source node transmits the data packets to the destination through the backbone route. Finally, the TB-RCBDT technique checks whether the PDR threshold was met during the data transmission process. If yes, the data transmission process is terminated. Otherwise, the RCBDT is retriggered to restart the packet transmission process. Algorithm 1 shows a step by step procedure of the design of the proposed TB-RCBDT technique.

```

Algorithm TB-RCBDT
{[Begin]
 Run MANET// Calling Algorithm MANET
 Source Node intends to send data packets to a destination node.
 RCBDT Algorithm triggered
 Through RCBDT algorithm Source node sends bait RREQ
 If (RREP from any node) {
do {
RCBDT algorithm tracks nodes that sent RREP and marks them as malicious
RCBDT algorithm blacklists any malicious node.
RCBDT algorithm deactivates blacklist nodes
RCBDT algorithm increases life bit of genuine
RCBDT algorithm calculates energy levels of genuine nodes
} while (Blackhole exists in MANET)
else {
 Source Node sends RREQ
 Destination node sends RREP//acknowledging to the source node
 OTB-DSR protocol calculates trust values for intermediates node that successfully passes RREQ packet to next-hop neighbor
 OTB-DSR protocol stores trust values in nodes caches
 OTB-DSR protocol uses cumulative trust values to calculate friendship level
 OTB-DSR protocol stores friendship level in nodes caches
 OTB-DSR protocol calculates Routes Trust Weights
 RCBDT algorithm and OTB-DSR protocol use the route selector module to establish the source routes from nodes cache that has the highest Route Trust Weight.
 Call SROC algorithm
 Established source route marked as backbone route
 Destination node sends data packets through the backbone route.
 while (not PDR threshold met) {
 go to RCBDT Algorithm triggered
 }
End Packet transmission
Release channel //bandwidth
Mark route as idle
}
[End]}

```

Algorithm 1: TB-RCBDT Algorithm



k) *Algorithm of SROC Module*

The SROC algorithm is used to select the most optimal source route. The algorithm first scans and creates an array of all possible routes in the source node cache. The routes are then compared based on their route trust values (RTVs). The source route with the highest RTV is selected and marked as the backbone

route to be used for packet transmission. However, if the backbone route proves to be invalid, the SROC algorithm refreshes the array. Further, the SROC algorithm restarts the process of selecting the backbone route afresh. The operations of the SROC algorithm are depicted in Algorithm 2.

```

Algorithm SROC ()
{
 int δmax // number of source routes in the cache array
 int backboneRoute
 Create S(δmax) // where S(δ) is an array of source routes, δ=10
 If S(δmax) > 1 {
 //Select δh , where δh is source route with highest CTV
 for (int i=0; i <= δmax-1; i++){
 if (δmax[i] > δmax[i+1]){
 δh = δmax[i]
 }
 }
 backboneRoute = δh
 if (δh -> Invalid)
 refresh (S(δmax))
 goto If S(δmax)
 else
 Transmit data
 }
}

```

Algorithm 2: SROC Algorithm

IV. SIMULATION ENVIRONMENT

To compare the effectiveness of the proposed TB-RCBDT technique, the simulation environment was setup in NS-3 Simulator. The simulation area measuring 1500 by 1000 meters was set in a rectangular pane. Additionally, fifty genuine mobile nodes were installed and configured. Further, two, four, and six blackhole nodes were installed in the three simulation scenarios. The black hole nodes used a simple attack model to entice other nodes in the network. The Channel of communication among nodes was set to User Datagram Protocol (UDP). OTB-DSR protocol was set as the routing protocol for all the nodes in the network.

For the nodes to manoeuvre within the simulation area, the propagation model was set to Radom Way Point (RWP) model. The nodes were configured using radio waves in a manner that could enable them to receive signals from all directions using an omnidirectional antenna. Constant Bit Rate (CBR) traffic model with a packet size of 512 bytes and sending rate of 4 packets per second was set to handle packet traffic. Simulation time for each scenario was set to 400 seconds. Finally, the nodes' transmission range was set to a radius of a radio range of 250 meters. Table 1 is a summary of the simulation parameters.

Table 1: Simulation Experiment Parameters

| Parameter                | Value                   |
|--------------------------|-------------------------|
| Channel Type             | Wireless Channel        |
| Simulation Time          | 400 seconds             |
| Number of nodes          | 50                      |
| MAC type                 | 802.11 IEEE             |
| Routing Technique        | TB-RCBDT                |
| Routing Protocol         | OTB-DSR                 |
| Movement Model           | Random Way Point        |
| Traffic model            | Constant Bit Rate (CBR) |
| Receiving Antenna        | Omnidirectional Antenna |
| Transport layer protocol | User datagram protocol  |
| Radio Transmission range | 250 meters              |

|                            |                    |
|----------------------------|--------------------|
| Packet size:               | 512 bytes          |
| Sending frequency          | 4 packets/second   |
| Simulation Area            | 1500*1000 meters   |
| Node speed                 | 1-10 meters/second |
| Number of black hole nodes | 2,4,5,6            |

## V. RESULTS AND DISCUSSIONS

The proposed TB-RCBDT technique was simulated in NS-3. Data generated by the Simulator was saved as text files of extension “.dat”. The text files were then executed using Gnuplot software to generate the output. The generated output was compared to the CBDS and ECBDS technique used as chosen

benchmarks. Packet delivery ratio, end-to-end delay, routing overhead, and energy consumption were the performance metrics in the experiment. Figure 4 shows the simulation environment of the RCBDT technique. The dots in red show the distribution of mobile nodes across the simulation area.

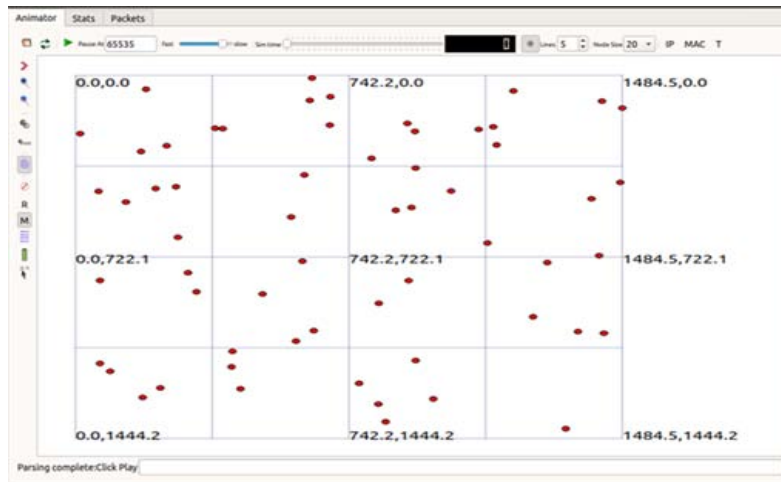


Figure 4: Simulation Interface for TB-RCBDT Technique

### a) Simulation Scenarios

The study comprised of four different simulation scenarios. Six simulation experiments were conducted in each scenario. The chosen scenarios represented real communication environments faced with security challenges. In each of the scenarios nodes' energy, nodes' speed, and the number of malicious nodes were varied and the performance of the proposed technique was observed. In the first scenario, the network had fifty genuine nodes. Further, one source node and one destination node were selected randomly. The source node was configured in a manner that it could request for packet transmission to the destination node through the proposed technique. The initial energy of nodes was set to 60 joules. Nodes' speed was set to 5 m/sec. Simulation time was set to 400 seconds while the traffic generation interval was set to 10 seconds. Further, the proposed technique was simulated in an ideal environment. In this experiment, two malicious nodes were introduced into the network. The performance of the proposed technique was evaluated against the three metrics in all the six experiments. An average of each metric in the six experiments was taken.

In the second scenario, one source node and two destination nodes were selected. The purpose of

increasing the destination nodes was to increase the degree of transmitted packets to black hole nodes. Further, four blackhole nodes were introduced in the simulation environment. The blackhole nodes represented adversaries in emergencies that thwart the communication process. In our experiment, blackhole nodes were used to lure the source node to channel packets through them during simulation experiments. The blackhole nodes would then drop the data packets. The nodes' speed was set to 10 m/sec. The initial energy of nodes was varied from 60 joules to 80 joules. Traffic generation was set to 20 seconds. Six simulation experiments were conducted in this scenario in the presence of two blackhole nodes. Further, the performance of the proposed technique was evaluated in the presence of the two blackhole nodes. The results of the three metrics were recorded. The effect of the two malevolent nodes was evaluated based on recorded results for each simulation experiment. Finally, an average of each metric in the six experiments was taken and compared to the results of scenario one.

In the third scenario, one source node and four destination nodes were selected randomly. Nodes' speed was set to 15 m/sec. Traffic generation was set to 30 seconds. The black hole nodes were increased to

five. The initial energy of nodes was varied from 80 joules to 90 joules.

Finally, in the fourth scenario, one source node and six destination nodes were selected randomly. Node speed was set to 20 meters per second, traffic generation was varied from 30 to 40 seconds, and black hole nodes were increased to six. The initial energy of nodes was varied from 90 joules to 100 joules.

b) *Analysis of Simulation Results*

i. *Packet Delivery Ratio*

Results from the simulation scenarios show that the packet delivery ratio of the proposed TB-RCBDT technique was superior compared to the benchmark technique. A summary of the packet delivery ratio simulation results of the proposed technique is illustrated in Tables 2.

Table 2: Results of Scenario for Packet Delivery Ratio

| Simulation Experiment | Scenario 1<br>Packet Delivery Ratio (%) | Scenario 2<br>Packet Delivery Ratio (%) | Scenario 3<br>Packet Delivery Ratio (%) | Scenario 4<br>Packet Delivery Ratio (%) |
|-----------------------|-----------------------------------------|-----------------------------------------|-----------------------------------------|-----------------------------------------|
| 1                     | 99.88                                   | 98.81                                   | 97.65                                   | 97.37                                   |
| 2                     | 99.88                                   | 98.55                                   | 97.34                                   | 98.08                                   |
| 3                     | 99.88                                   | 99.08                                   | 97.97                                   | 97.74                                   |
| 4                     | 99.88                                   | 98.42                                   | 97.18                                   | 97.04                                   |
| 5                     | 94.88                                   | 99.47                                   | 98.44                                   | 95.43                                   |
| 6                     | 99.88                                   | 98.68                                   | 99.06                                   | 96.91                                   |
| Average               | 99.88                                   | 98.84                                   | 97.94                                   | 97.76                                   |

The minimum packet delivery ratio of the TB-RCBDT technique was 94% which was recorded in scenario 1. This was attributed to the low energy levels of the nodes in the network. When the energy levels of some nodes went low, they behaved selfishly by not forwarding some packets to their intermediate nodes in the route. The selfish act made these nodes to save energy to extend their lifetime in the network.

The proposed technique recorded a higher packet delivery ratio of 99% in scenario 1 as indicated in Figure 5 despite the presence of cooperative blackhole nodes. In this scenario nodes' speed was 5 meters per second. However, scenario 4 had a lower packet delivery ratio despite higher energy levels. This implies that the higher the nodes speed, the more the energy it consumes during its mobility hence making it behave selfishly as the battery depletes. Although scenario 4 had enough energy to sustain packet transmission in the network, most of the energy was used in mobility due to high speed. This explains why the packet delivery ratio of scenario 1 was higher than that of scenario 4.

On average in all the four scenarios, TB-RCBDT had a higher packet delivery ratio than ECBDS and CBDS used as benchmark techniques. This was attributed to the fact that the proposed technique uses the concept of trust among intermediate nodes to determine which nodes are genuine in the network. Nodes that have successfully passed data packets to their immediate neighbours in the past are regarded as 'trusted'. The trusted nodes are the ones that form source routes in the proposed technique. This implies that despite the higher numbers of malicious nodes in the network, the TB-RCBDT technique is resilient

enough to transmit data packets with minimal loss and at a percentage of over 95%.



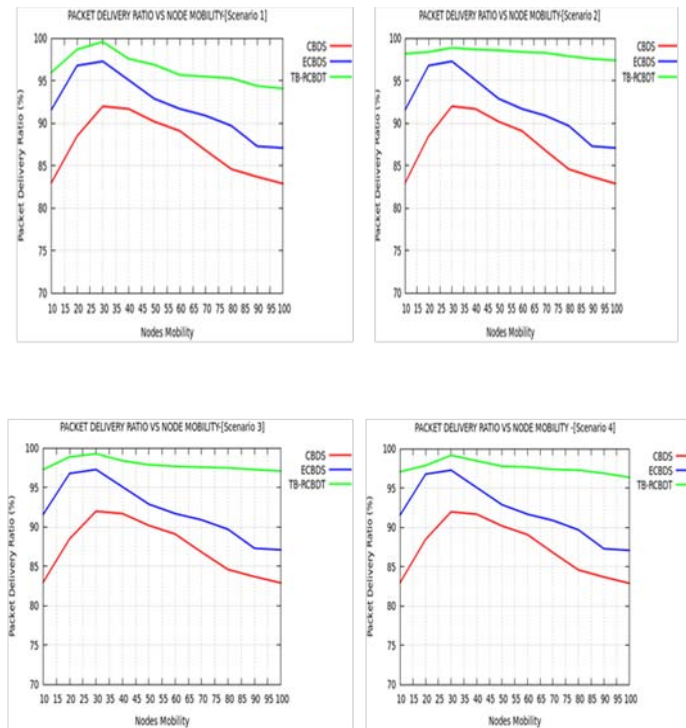


Figure 5: Packet Delivery Ratio Vs Nodes Mobility for Scenarios 1 to 4

ii. End to End Delay

The results of all simulation experiments in the four scenarios were captured in Table 3. As indicated from the table, the end-to-end delays gradually increased from experiment one to experiment six for all the simulation scenarios. The end-to-end delay is a product of turnaround time. Turn-around time is the time taken between the request of transmission by the source node and the grant of the request by the destination node.

The gradual increase of end-to-end delay was attributed to increased nodes in packet transmission.

Hence a lot of time was used in making forwarding decisions. However, generally, on average, the end-to-end delay reduced from scenario one to scenario four. This was attributed to the fact that as the nodes energy increased from scenario one to four, very few nodes were willing to act selfishly during packet transmission. This reduced the time taken during the establishment of source routes. For instance, in scenario one the minimum end-to-end delay was 0.3332 seconds in experiment one while the maximum was 0.3529 seconds in experiment six.

Table 3: Results of Scenario for End to End Delay

|                       | Scenario 1             | Scenario 2             | Scenario 3             | Scenario 4             |
|-----------------------|------------------------|------------------------|------------------------|------------------------|
| Simulation Experiment | End-to-End Delay (Sec) | End-to-End Delay (Sec) | End-to-End Delay (Sec) | End-to-End Delay (Sec) |
| 1                     | 0.3332                 | 0.3544                 | 0.3612                 | 0.3822                 |
| 2                     | 0.3372                 | 0.3623                 | 0.3734                 | 0.3798                 |
| 3                     | 0.3417                 | 0.3571                 | 0.3699                 | 0.3875                 |
| 4                     | 0.3526                 | 0.3649                 | 0.3711                 | 0.3894                 |
| 5                     | 0.3522                 | 0.3583                 | 0.3687                 | 0.3912                 |
| 6                     | 0.3529                 | 0.3682                 | 0.3706                 | 0.3785                 |
| Average               | 0.35                   | 0.3609                 | 0.3691                 | 0.3848                 |

The proposed technique had the lowest end-to-end delay of 0.35 seconds as indicated in Figure 6. On average, in all the simulation scenarios the benchmark techniques ECBDS and CBDS had minimum end-to-end delays of 0.58 and 0.61 seconds respectively. Further, it was observed that as the number of nodes increased in the network; there was a proportionate increase of end-

to-end delay in all the techniques. The proportionate increase of end-to-end delay was attributed to the fact that every node took some time to make a routing decision. However, since in the proposed TB-RCBOT technique nodes had already been prequalified based on Composite Trust Values (CTV) and social groups, there was a negligible time used on every node in the

selected source route. This implies that the proposed TB-RCBDT had the shortest turn-around time.

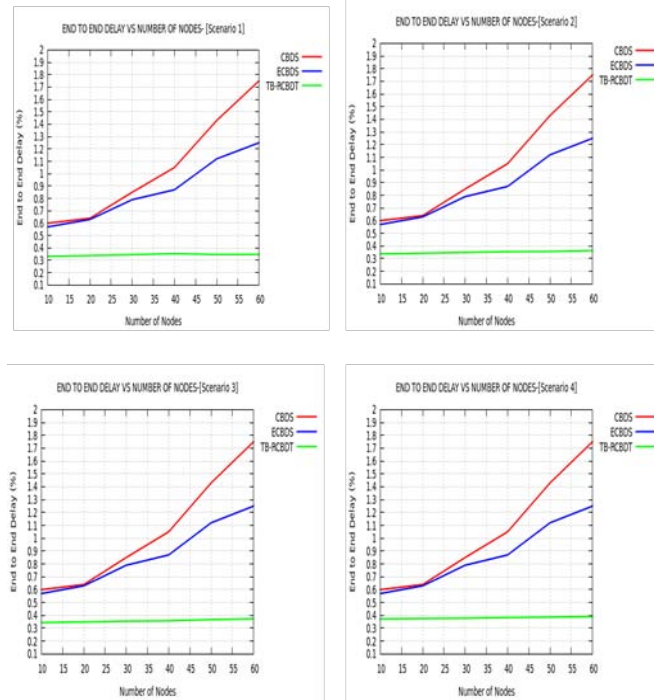


Figure 6: Graph of End to End Delay Vs Number of Nodes for Scenarios 1 to 4

c) Routing Overhead

Routing overhead is a ratio that represents the number of controls packets versus the number of data packets sent in every data frame. Table 6 represents the summarized results of the routing overhead for the four simulation scenarios. The columns in the table represent the simulation scenarios while the rows represent the number of experiments per scenario. Simulation results

show that the routing overhead of the TB-RCBDT technique increased gradually from scenario one to scenario four. For instance, scenario, one had an average of 3.965% while scenario four had an average of 5.549 %. However, it was observed that the TB-RCBDT technique had the lowest routing overhead of between 4 and 5.5% as indicated in Table 4.

Table 4: Results of Scenario for Routing Overhead

|                              | Scenario 1              | Scenario 2              | Scenario 3              | Scenario 4              |
|------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| <b>Simulation Experiment</b> | <b>Routing Overhead</b> | <b>Routing Overhead</b> | <b>Routing Overhead</b> | <b>Routing Overhead</b> |
| 1                            | 3.974                   | 4.135                   | 4.238                   | 5.433                   |
| 2                            | 3.958                   | 4.142                   | 4.243                   | 5.451                   |
| 3                            | 3.965                   | 4.137                   | 4.268                   | 5.449                   |
| 4                            | 3.979                   | 4.139                   | 4.255                   | 5.452                   |
| 5                            | 3.948                   | 4.161                   | 4.273                   | 5.537                   |
| 6                            | 3.964                   | 4.153                   | 4.249                   | 5.573                   |
| Average                      | 3.965                   | 4.145                   | 4.254                   | 5.549                   |

This was significantly small compared to the benchmark techniques. ECBDS had a minimum of 5% and a maximum of 15%, while CBDS had a minimum of 5.55 and a maximum of 17%.

It was noted that in all the scenarios, as the number of cooperative blackholes increased, routing overhead proportionally increased for the three techniques. An increase in routing overhead was attributed to the increase in cooperative blackhole

nodes. The extra overhead requires the routing technique to make informed decisions when selecting nodes to participate in packet routing. This translates to an increased number of control packets.

However, the proportionate increase in routing overhead for the proposed TB-RCBDT was small in all the cases as indicated in Figure 7. This was attributed to the fact that the proposed technique only selected the highest priority source route. High priority source routes

have minimal chances of having malicious or selfish nodes. This implies that the proposed TB-RCBDT is more efficient in packet delivery compared to the

benchmark techniques as it only used a few control packets.

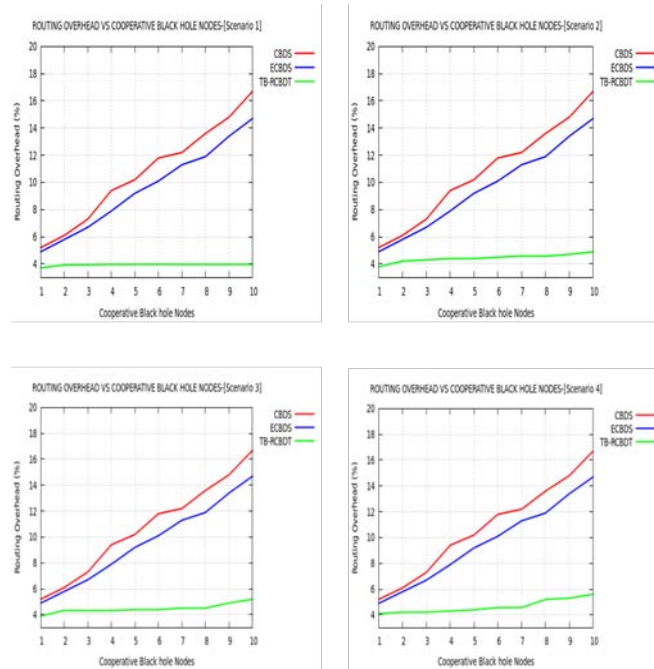


Figure 7: Routing Overhead Vs Cooperative BlackHole Nodes for Scenarios 1 to 4

d) Energy Consumption

As opposed to wired networks, nodes in MANETs are always in motion. This means that at any given time a node keeps on changing its geographical location. These nodes have inbuilt rechargeable batteries in their architecture. The batteries enable them to supply energy as they manoeuvre across the network. However, the depletion of energy levels in the batteries is directly proportional to nodes' mobility and the levels of engagement in packet transmission.

As nodes transmit packets and manoeuvre through the network, they consume a lot of energy. In this study, the consumption of energy by nodes was captured in all the simulation scenarios. Table 5 is a summary of the results of the nodes' final energy in the four simulation scenarios. The initial nodes' energy for the four scenarios was 60 joules, 80 joules, 90 joules, and 100 joules respectively.

Table 5: Results of Scenario for Energy Consumption

| Simulation Experiment | Scenario 1<br>Nodes' Final Energy | Scenario 2<br>Nodes' Final Energy | Scenario 3<br>Nodes' Final Energy | Scenario 4<br>Nodes' Final Energy |
|-----------------------|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| 1                     | 49.256                            | 65.78                             | 68.34                             | 73.47                             |
| 2                     | 49.434                            | 66.39                             | 69.18                             | 74.39                             |
| 3                     | 49.389                            | 64.99                             | 68.76                             | 73.58                             |
| 4                     | 49.167                            | 65.64                             | 69.23                             | 73.82                             |
| 5                     | 49.336                            | 66.47                             | 68.65                             | 74.14                             |
| 6                     | 49.249                            | 65.68                             | 68.52                             | 74.26                             |
| Average               | 49.356                            | 65.82                             | 68.78                             | 73.94                             |

In scenario one, on average the nodes' battery depleted by 11 joules; that is from 60 joules to 49.356 joules. Further, in scenario four on average the nodes' battery depleted by 26 joules; that is from 100 joules to 73.94 joules. The increase in battery energy depletion was noted across the four simulation scenarios. This was attributed to the increased number of cooperative

blackhole nodes in the network. Table 5 shows that there is a direct correlation between the increase in the number of black hole nodes and the increase in depletion levels of nodes' battery power. This is an indication that the cooperative blackhole nodes constantly drain nodes' battery energy to bring down the network. However, it was observed that the proposed

TB-RCBDT technique had the lowest energy consumption levels of between 49 and 73.9 Joules as indicated in the table.

Figure 8 is a graph of nodes' energy versus simulation time (in seconds) for the four simulation scenarios. In the four simulation scenarios, the nodes' initial energy was set to 60 joules, 80 joules, 90 joules, and 100 joules respectively as indicated in the figure. The energy consumption of the proposed TB-RCBDT is indicated in green colour while that of ECBDS and CBDS are indicated in blue and red colour respectively.

The results of the four simulation scenarios indicate that there is an inverse correlation between nodes' energy and the simulation time for the three techniques. As the simulation time increases, the nodes' energy levels decrease proportionally. However, from the figure, it can be noted that the proposed TB-RCBDT technique had the lowest nodes' energy utilization levels compared to CBDS and ECBDS techniques. This is an indication that the TB-RCBDT technique is more efficient in terms of energy consumption.

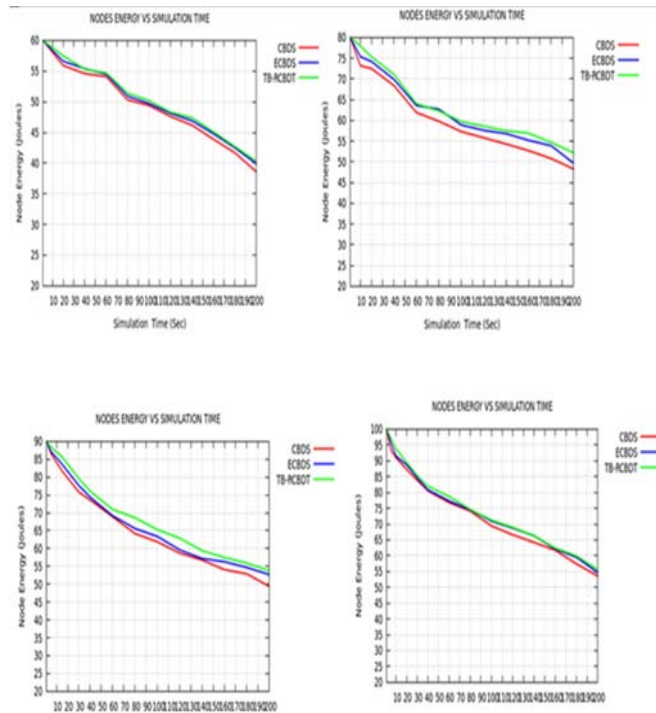


Figure 8: Node Energy Vs Simulation Time for Scenarios 1 to 4

## VI. CONCLUSION AND FUTURE WORK

MANETs are wireless networks that have attracted attention from various domains due to their flexibility and ease of deployment. However, MANETs are prone to a range of security threats. Security is a key concern in any communication system. Guaranteeing security in MANETs is today's one of the biggest challenges. The study proposed a TB-RCBDT technique against cooperative black hole attacks in MANETs. Simulation results indicated that the proposed TB-RCBDT technique is superior to both CBDS and ECBDS used as benchmark techniques. Performance metrics used include; packet delivery ratio, end-to-end delay, routing overhead, and energy consumption. This implies that the proposed TB-RCBDT technique is resilient and robust in mitigating cooperative black hole attacks in MANETs. TB-RCBDT technique has the capability of maintaining better performance through the transmission process as compared to benchmark techniques.

As part of our future work, we intend to improve the TB-RCBDT technique by incorporating an element of artificial intelligence using fuzzy logic. This will improve the effectiveness and efficiency of the technique in mitigating cooperative black hole attacks.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Rutvij, H., Jhaveri, J., Sankita, P., Jinwala, C. D.: 'A Novel Solution for Gray hole Attack in AODV Based MANETs', In Proc. of Third International Conference on Advances in Communication, Network and Computing: Springer, 2012, pp.60-67.
2. Boukerche, A. et al.: 'Routing protocols in Ad-hoc networks: a survey of Computer Networks', 2011, 55(13), pp. 3032–3080.
3. Jeenat, S., Tasnuva, A.: 'Securing AOMDV Protocol in Mobile Ad-hoc Network with Elliptic Curve Cryptography', International Conference on Electrical, Computer and Communication Engineering (ECCE), IEEE, 2017, pp. 539-543.



4. Sagar, R. D. Chatur, P. N., Nikhil, B. B.: 'AODV-Based Secure Routing Against Blackhole Attack in MANET', IEEE International Conference on Recent Trends in Electronics Information Communication Technology, IEEE, 2016, pp. 319-326.
5. Soufiene, D. Farid, N. Zonghua, Z.: 'Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks: Proposals and Challenges', IEEE Communications Surveys & Tutorials, 2011, 13(4), pp. 658 – 672.
6. Abdelshafy, M. A., King, P. J. B.: 'Resisting Blackhole Attacks on MANETs', 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2016, pp. 1048 – 1053.
7. Sukanesh, R., Edsior, E., Aarthylakshmi, M.: 'Energy Efficient Malicious Node Detection Scheme in Wireless Networks', IEEE, 2016, pp. 307-312.
8. Sen, J. Koilakonda, S., Ukil, A.: 'A mechanism for detection of Co-operative Black hole attack in Mobile Ad-hoc networks', Second International Conference on Intelligent Systems, Modeling and Simulation, IEEE, 2011, pp. 338-343.
9. Mistry, N., Jinwala, D. C., Zaveri, M.: 'Improving AODV Protocol against Blackhole Attacks', International Multiconference of Engineers and Computer Scientists, 2010, 2(6), pp. 1-6.
10. Su, M-Y., Chiang, K-L., Liao, W-C.: 'Mitigation of Black-Hole Nodes in Mobile Ad-hoc Networks', International Symposium on Parallel and Distributed Processing with Applications, IEEE, DOI:10.1109/ISPA.2010.74, 2010, pp. 105-113.
11. Gupta, S., Kar, S., Dhararaja, S.: 'BAAP: Blackhole Attack Avoidance Protocol for Wireless Network', International Conference on Computer & Communication Technology (ICCT), IEEE, 2011, pp.1-6.
12. Saha, H. N., et al.: 'Two-level Secure Re-routing (TSR) in Mobile Ad-hoc Networks', IEEE, DOI 10.1109/MNCAppls.2012.31, 2012, pp. 119-122.
13. Bhosle, A. A., Thosar, T. P., Mehatre, S.: 'Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET', International Journal of Computer Science, Engineering and Applications (IJCSEA), 2012, 2(1), pp. 45-54.
14. Thachil, F., Shet, K. C.: 'A trust-based approach for AODV protocol to mitigate Black hole attack in MANET', International Conference on Computing Sciences, IEEE, 2012, pp. 312-325.
15. Bindra, G. S., et al.: 'Detection and Removal of Co-operative Blackhole and Gray hole Attacks in MANETs', IEEE, 2012, 3(11), pp. 207-212.
16. Ukey, A. S. A., Chawla, M., Singh, V. P.: 'I-2ACK: Preventing Routing Misbehavior in Mobile Ad-hoc Networks', International Journal of Computer Applications (0975-8887), 2013, vol. 62(12), pp.345-353.
17. Hiremani, V. A., Jadhao, M. M.: 'Eliminating Co-operative Blackhole and Gray hole Attacks Using Modified EDRI Table in MANET', IEEE, DOI:10.1109/ICGCE.2013.6823571, 2013, pp. 944-952.
18. Gaikwad, V., Ragha, L.: 'Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET', International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE, 2015, pp.306-311.
19. Dumne, P. R., Manjaramkar, A.: 'Cooperative Bait Detection Scheme to prevent Collaborative Blackhole or Gray hole Attacks by Malicious Nodes in MANETs', 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), IEEE, 2016, pp. 486-490.
20. Emimajuliet, P., Thirilogasundari, V.: 'Defending Collaborative Attacks in MANETs Using Modified Cooperative Bait Detection Scheme', International Conference On Information Communication And Embedded System (ICICES), ISSN: 978-1-5090-2552-7, 2016, pp. 819-826.
21. Allard, G. P., et al.: 'Evaluation of the energy consumption in MANET', Adhoc-Now, Ottawa, Canada, 2006, pp. 41-51.
22. Bheemalingaiah, M., Naidu, M. M., Rao, D. S.: 'Energy-aware Clustered based Multipath Routing in Mobile Ad-hoc Networks', *International Journal of Communications, Network and System Sciences*, 2017, 2(5), pp. 1-24.
23. Cao, L., Dahlberg, T., Wang, Y.: 'Performance evaluation of energy-efficient Ad-hoc routing protocols', *Proc. IPCCC, IEEE*, 2007, pp. 306-313.
24. Rango, F., Guerriero, F., Fazio, P.: 'Link-Stability and Energy-aware Routing Protocol in Distributed Wireless Networks', *Journal of IEEE Transaction on Parallel and Distributed Systems*, 2012, pp. 347-362.
25. Dorri, A., Kamel, S. R., Kheyrikhah, E.: 'Security Challenges in Mobile Ad-hoc Networks: A Survey', *International Journal of Computer Science & Engineering Survey (IJCSES)*, 6(1), pp. 15-29, DOI:10.5121/ijcses.2015.6102, 2015.
26. Guo, Z., Malakooti, B.: 'Energy-Aware Proactive MANET Routing with Prediction on Energy Consumption', *International Conference on Wireless Algorithms, Systems and Applications*, IEEE, DOI: 10.1109/WASA.2007.151, 2007, pp. 287-292.
27. Shabbir, A., et al.: 'Security: A Core Issue in Mobile Ad-hoc Networks', *Journal of Computer and Communications*, <http://dx.doi.org/10.4236/jcc.2015.312005>, 2015, 3(3), pp.41-66.
28. Toh, C. K.: 'Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless





Ad-hoc Networks, Communication Magazine', *10th International Conference on Practical Applications of Agents and Multi-Agent Systems*, IEEE, 2001, 39(6), pp. 174-186.

29. Mwangi, E. G., Muketha, G. M., Kamau, G. N.: 'Design and Implementation of Resilient Cooperative Bait Detection Technique to Curb Cooperative Black Hole Attacks in MANETs Using DSR Protocol', *International Journal of Networks and Communications* DOI: 10.5923/j.ijnc.20201001.01. 2020, 10(1), pp.1-9, 2020.
30. Mwangi, E. G., Muketha, G. M., Kamau, G. N.: 'Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3', *International Journal of Networks and Communications*, DOI: 10.5923/j.ijnc.20201001.02. 2020, 10(1), pp.10-19.





## BER Performance Analysis of OFDM, W-OFDM and F-OFDM for 5G Wireless Communications

By MD. Hasan Mahmud, Mirza Abir Mahmud, MD. Hafizul Islam  
& MD. Maruf Hosain

*Pabna University*

**Abstract-** Orthogonal Frequency Division Multiplexing (OFDM) is a pertinent multi-carrier modulation approach that is more immune to frequency selective fading. In the 5G waveform, in order to reduce the traffic in OFDM based on technology, it is important to re-size the bandwidth. Consequently, a spectrally localized waveform technology called Filtered Orthogonal Frequency Division Multiplexing (F-OFDM), which is primarily an approach to sub-band based filtering is introduced. Windowed-OFDM (W-OFDM), which is basically a classical OFDM scheme where each symbol is windowed and overlapped in the time domain. Each of the different sub-bands can be processed according to the traffic scenario. This paper presents the comparison of the performance analysis of MIMO-OFDM, MIMO-WOFDM, and MIMO-FOFDM systems using BPSK, QPSK, 16-PSK, QAM, 8-QAM and 16-QAM modulation techniques under Rayleigh fading channel.

**Keywords:** OFDM, F-OFDM, W-OFDM, relay, MIMO, BPSK, QAM, BER, ISI.

**GJCST-E Classification:** C.2.1



*Strictly as per the compliance and regulations of:*



# BER Performance Analysis of OFDM, W-OFDM and F-OFDM for 5G Wireless Communications

MD. Hasan Mahmud <sup>α</sup>, Mirza Abir Mahmud <sup>ο</sup>, MD. Hafizul Islam <sup>ρ</sup> & MD. Maruf Hosain <sup>ω</sup>

**Abstract-** Orthogonal Frequency Division Multiplexing (OFDM) is a pertinent multi-carrier modulation approach that is more immune to frequency selective fading. In the 5G waveform, in order to reduce the traffic in OFDM based on technology, it is important to re-size the bandwidth. Consequently, a spectrally localized waveform technology called Filtered Orthogonal Frequency Division Multiplexing (F-OFDM), which is primarily an approach to sub-band based filtering is introduced. Windowed-OFDM (W-OFDM), which is basically a classical OFDM scheme where each symbol is windowed and overlapped in the time domain. Each of the different sub-bands can be processed according to the traffic scenario. This paper presents the comparison of the performance analysis of MIMO-OFDM, MIMO-WOFDM, and MIMO-FOFDM systems using BPSK, QPSK, 16-PSK, QAM, 8-QAM and 16-QAM modulation techniques under Rayleigh fading channel. The main aim of this paper is to focus on analyzing the performance of OFDM, W-OFDM, and F-OFDM in terms of Power Spectral Density (PSD), Bit error rate (BER) and signal to noise ratio. The spectral efficiency in F-OFDM is dramatically increased by the reduction of out-of-band (OOB) emission rather than OFDM and W-OFDM. Simulation for the performance analysis of OFDM, W-OFDM, and F-OFDM is represented in terms of PSD and BER have done in MATLAB.

**Keywords:** OFDM, F-OFDM, W-OFDM, relay, MIMO, BPSK, QAM, BER, ISI.

## I. INTRODUCTION

After years of discussions through the industry and academia, the requirements and expectations for the 5th generation (5G) cellular networks have been made clear. Whilst the millimeter wave is expected to deliver short-range with high-speed radio access by tens of Gbps the lower frequency bands (e.g., those are currently used by the 4G long-term evolution networks) will continue to provide ubiquitous and reliable radio access, but with an improved spectrum efficiency [1]. To this end, the air interface, mainly the underlying waveform, should be revisited. Next-generation cellular networks present the most challenging issues for researchers and engineers.

The main aim is to improve the actual LTE performance, in order to meet the growing data demand from the newly provisioned technologies and services [2]. For instance, increasing the data rate by a factor 100 with respect to LTE, while decreasing the latency from the actual 15 ms down to as low as approximately,

*Author α σ ρ ω: Student, Department of information and communication engineering, Pabna university of science and technology. e-mails: jibonpustice@gmail.com, bokachoda@gmail.com, mankirpo@gmail.com, jsure@gmail.com*

1 ms. Massive MIMO Enabling new technologies and services, such as Device-to-Device communications (D2D), Wireless Software Defined Networking (WSDN), Millimeter Wave communications and network Densification, are being utilized in order to reach 5G's goals [3] [4].

In this paper, we deal with problems concerning Radio Access techniques. As stated earlier, new services in 5G require high data rates with large spectral efficiency. For this reason, we focus on the spectral efficiency problem of a legacy the Orthogonal Frequency Division Multiplexing (OFDM) system, which has to improve its performance to achieve the required goal. As is well known, OFDM is the most important transmission technique of the recent past, largely used in LTE standards [5]. The principle of OFDM based on sub-carrier the division has been well studied and performed during the years and the first advantage of this scheme is its simplicity of implementation. Moreover, OFDM allows for simple modulation and demodulation and is highly MIMO friendly. On the other side, OFDM suffers from high PAPR (Peak-to-Average Power Ratio) and most of high Out-Of-Band (OOB) emissions. The required Cyclic Prefix (CP) and strict bounds for synchronization are other disadvantages of OFDM. Indeed, in a 5G scenario, it is desirable to use sub-bands that do not need to be perfectly synchronized with each other due to the different requirements of the multitude of devices on the network. In fact, in 5G we will have different kinds of devices that rarely connect to the network [5] [6]. For instance, an IoT (Internet of Things) device needs to send a few control bytes on rare occasions, and several kinds of devices will have a very short battery life. For these causes, it may be desirable to use a waveform with relaxed synchronization requirements [7].

This article attempts to summarize benefits and disadvantages of these two schemes currently being considered by 3GPP (Third Generation Partnership Project) for 5G applications, namely F-OFDM (Filtered OFDM) and W-OFDM (Windowed OFDM) based one BER, PSD and signal to noise ratio using BPSK, QPSK, 16-PSK, QAM, 8-QAM and 16-QAM modulation, we consider standard OFDM sub-bands, without using any strategy to reduce OOB emissions [8]. In the F-OFDM schemes, we consider low-pass filters in order to attenuate the OOB emissions and have an efficient sub-band divided system [9]. In the W-OFDM scenario, OOB

emissions are reduced by smoothing the symbol transitions with a time domain window applied on each sub-band. Other results on f-OFDM can be found in the [10], which gives a closed form for ISI (Inter-Symbol Interference), ICI (Inter-Carrier Interference) and ACI (Adjacent-Channel Interference). Suggests a filter-bank version of f-OFDM, while discusses PAPR reduction in F-OFDM.

## II. OFDM (ORTHOGONAL FREQUENCY-DIVISION MULTIPLEXING)

OFDM means Orthogonal frequency-division multiplexing. OFDM scheme requires N number of sub-carriers to transmit the number of data streams. Each of these carriers is orthogonal to other and centered at multiples of frequencies. These serial data streams are converted to N parallel data streams and then they are digitally modulated using appropriate modulation techniques like BPSK, QAM, PSK and others [11]. The constellation mapper or Lookup Table is used for the special purpose that is the modulation. For the superimposition of the modulated data on the orthogonal sub-carriers, it demands N sinusoidal oscillators tuned with N orthogonal frequencies that are parallel to each other.

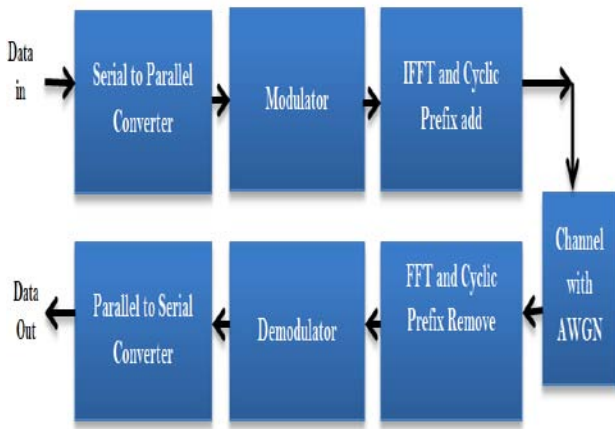


Figure 1: OFDM Architecture

The output of the sinusoidal oscillators is added up together that results to produce an final OFDM signal. These oscillators and the summer are replaced with an IFFT block that was recommended by Weinstein and Ebert to scale down the complexity of OFDM [11] [12]. From the IFFT output, the OFDM symbol samples are attained. The IFFT block switches the signal from frequency domain to time domain. Fig. 1 above shows the OFDM Architecture.

The Inter-symbol-Interference (ISI) imposes a negative impact on the OFDM which is induced by the specific delay spread. Delay spread occurs since multiple copies of the transmitted signals are received at different intervals of time rather than a single time. But the ISI results when the delay spread goes beyond the

symbol time duration. The ISI can be eliminated by the use of the cyclic prefix [12]. The cyclic prefix is a manner of adjoining some portion of the OFDM symbol at the beginning of the OFDM symbol. The Inter-carrier-interference (ICI) can also be eliminated by the proper use of the cyclic prefix. The channel portion adds AWGN (Additive White Gaussian noise) to the received signal. The reverse operation of transmitter section appears at the receiver side. At the receiver section, the transmitted signal is converted from analog to digital and then removes the cyclic prefix portion. The receiver has to perform synchronization (both channel timing and frequency), channel estimation, demodulation, and decoding systems. The output from FFT and the input of the IFFT are same range [13] [14]. Finally, the original signal can be recovered by reassembling all data streams from the individual carrier.

## III. WINDOWED OFDM (W-OFDM)

In this section, we illustrate time domain windowing strategy. Since, the signal high frequency components are generated by the discontinuities between adjacent OFDM symbols, softening these singularities with a proper transition lowers the OOB emissions [10].

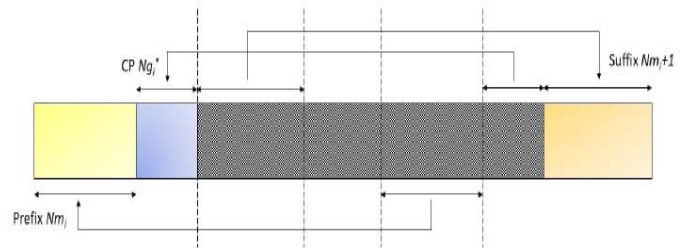


Figure 2: CP, prefix and suffix extension for a W-OFDM symbol

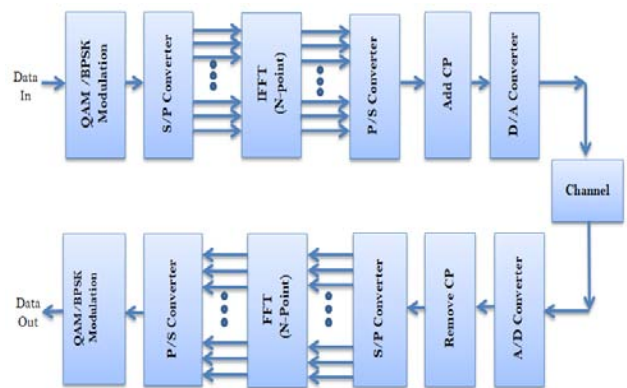


Figure 3: W-OFDM Architecture

The OFDM symbols must be elongated with the insertion of CP, prefix and suffix, then windowed and finally concatenated (by partially overlapping two consecutive symbols) according to fig.2. W-OFDM Architecture model is denoted by fig.3.

The first operation is to extend the OFDM symbol by copying the last  $N_{gi}$  samples of the native OFDM symbol at the beginning of the new W-OFDM symbol, as typically done for CP-OFDM [15]. The first  $N_{mi}$  samples are denoted as “prefix”, while the remaining  $N_{gi}$  are denoted by CP. The W-OFDM symbol is then further extended by copying the first  $N_{mi} + 1$  samples of the native OFDM symbol at the end of the new W-OFDM symbol, as shown in the Figure. Native OFDM symbols in each sub-band may have different lengths; hence the parameter  $N_{mi}$  is used to denote the prefix or suffix parameter for the  $i^{th}$  sub-band. At this point the W-OFDM symbol that is denoted as  $X_i$  contains  $N_i^W = N_i + N_{gi} + 2N_{mi} + 1$  samples [16]. However, prefix and suffix both will be smoothed with a windowing operation, and then the suffix of the  $i^{th}$  W-OFDM symbol will be overlapped with the first  $N_{mi} + 1$  samples of the  $(i+1)^{th}$  W-OFDM symbol. The windowed symbol  $x_m$  is obtained from the extended symbol  $x$  via equation (1).

$$x_m = x_i \cdot w_i \tag{1}$$

Where,  $w_i$  represents the window of length  $N_i^{(w)}$ . We use a window defined via equation (2).

$$w_i = \begin{bmatrix} 0^{(N_{mi} - N_{tri} / 2)} \\ 1^{(N_i + N_{gi} - N_{tri} + 1)} \\ 0^{(N_{mi} - N_{tri} / 2)} \end{bmatrix} \tag{2}$$

Where,  $0^L$  represents a column vector of  $L$  elements filled by zeros, likewise  $1^L$  is the similar type of vector filled by ones. The parameter  $N_{tri}$  represents the window transition length, i.e. the number of samples the window spends to go from zero-to-one and from one-to-zero,  $N_{ri}$  is the transition length in the  $i^{th}$  of sub-band.

#### IV. FILTERED OFDM (F-OFDM)

The transmission chain for f-OFDM is similar to that for the CP-OFDM, with an additional low-pass filter introduced

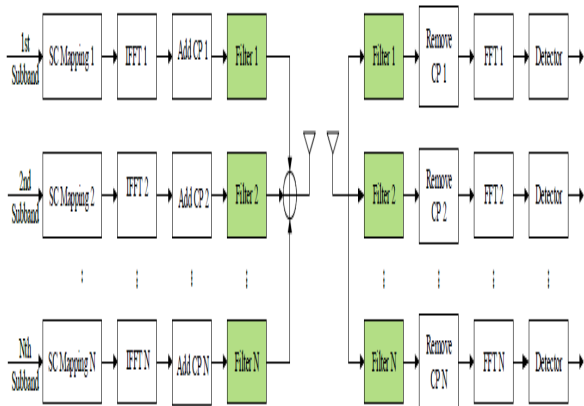


Figure 4: Downlink transceiver structure of F-OFDM

After the CP concatenation and the frequency shift in order to reduce the OOB emissions. Downlink transceiver structure of F-OFDM. is denoted by fig.4. Clearly, the structure of the transmitter low-pass filter is numerous important for reducing OOB emissions and possible interference. we want a filter perfectly flat in pass-band and zero outside this band, with null transition bands [17] [18]. This kind of filter is unrealizable but can be approximated by truncating and windowing the ideal sinc (.) impulse response. This operation introduces the new element in this framework, the filter transition bands. It is important to note that the transition bands are completely independent of frequency guard bands. Obviously having the transition band contained in the guard band could guarantee better performances. The filter has to be as flat as possible in the pass-band with tight transition bands section. To achieve this specific goal we have chosen a windowed-sinc filter with ideal impulse response

$$p_i(n) = \text{Sinc}(\Delta f_i(N_{ui} + 2R_i) n / N_i) \tag{3}$$

For  $-[L_i/2] \leq n \leq [L_i/2]$ , Where  $L_i$  represents the filter order and  $\Delta f_i R_i$  the transition band in one side.  $p_i(n)$  doesn't represent our final filter, it is only a truncated based sinc. The Role of transition bands of the filter is given below by the fig.5.

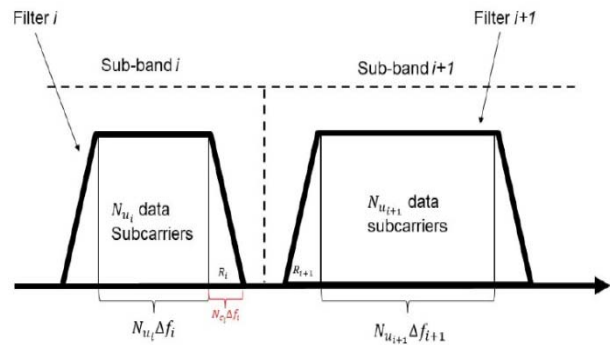


Figure 5: Role of transition bands of the filter

The final coefficients of our normalized low pass filters are given by the equation (4).

$$f_i(n) = \frac{p_i(n) \cdot w_i(n)}{\sum_k p_i(k) \cdot w_i(k)} \tag{4}$$

$$w_i(n) = (0.5(1 + \cos(\frac{2\pi n}{L_i - 1})))^{0.5} \tag{5}$$

Where,  $n$  is bounded as in equation. The filter impulse response contains  $2L_i + 1$  samples, that causes a signal extension in the time domain by  $2L_i$  samples. Fortunately, this kind of filter has the major part of its energy concentrated in the Sinc lobe, so the elongation is important just for a small time period during the CP of the symbol [19]. For this reason, it is not necessary to choose  $L_i$  to be very small, specifically  $L_i$  can be larger than  $L_{gi}$  (length of the cyclic prefix).



V. SYSTEM MODEL

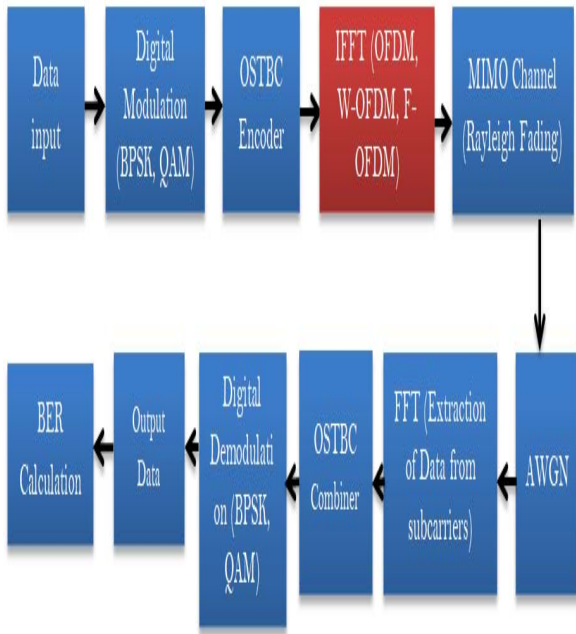


Figure 6: MIMO incorporated OFDM, WOFDM and F-OFDM wireless system

The MIMO incorporated OFDM, W-OFDM and F-OFDM-WOFDM systems are modeled using Orthogonal Space Time Block Coding (OSTBC) technique, having symbol wise maximum likelihood (ML)

decoding, to attain the high diversity gains in order to obtain higher data rates. The proposed system model is demonstrated in Fig.6. For simulation, the random binary signal is created and modulated by employing the different modulation techniques such as BPSK, QPSK, 16-PSK, QAM, 8-QAM and 16-QAM. The signals are encoded via orthogonal space time block codes for transmission over the Rayleigh fading channel. Five independent antennas links are formed, out of which four are served as transmitting antennas and the remaining four are acting as receiving antennas. During the transmission through the channel, IDWT transformation is performed after the OSTBC encoding. For W-OFDM transmission, the information is first grouped and mapped according to the modulation and then, is sent to inverse discrete wavelet transform (IDWT), which converts frequency domain signal into time domain signal and also provides orthogonality similarly for F-OFDM. The simulation adds white the Gaussian noise at the receiver process. Then, it combines the signals from both receive antennas into a single stream for the demodulation. Afterward, DWT is applied at the receiver side to reconstruct the signal in frequency domain. Total of 192 Samples per frame have been taken. Bits per symbol considered for the simulation is 100. W-OFDM and F-OFDM symbol rates are 10Ksps and the symbol period is 10-6s. The system is designed over four transmitting antennas and four receiving antennas (4 x 4) employing an independent Rayleigh fading for transmission of data.

VI. RESULTS AND ANALYSIS

Table 1: Summary of Simulated Model Parameters

| Parameter                                | Considerations for Simulation             |
|------------------------------------------|-------------------------------------------|
| Modulation Scheme                        | BPSK, QPSK, 16-PSK, QAM, 8QAM, and 16-QAM |
| Channel                                  | Rayleigh Fading Channel                   |
| Multiplexing                             | OFDM, W-OFDM, F-OFDM                      |
| Samples per frame                        | 192                                       |
| No. of transmitting & receiving antennas | 4*4                                       |
| Signal to Noise Ratio                    | 0 to 25dB                                 |



PSD -40  
dB

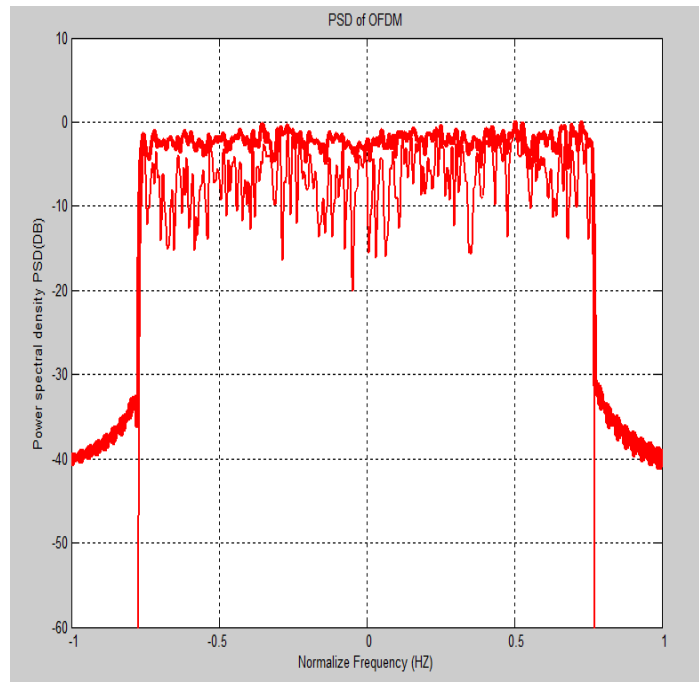



Figure 7: Power spectral density (PSD) of OFDM.

PSD -50  
dB

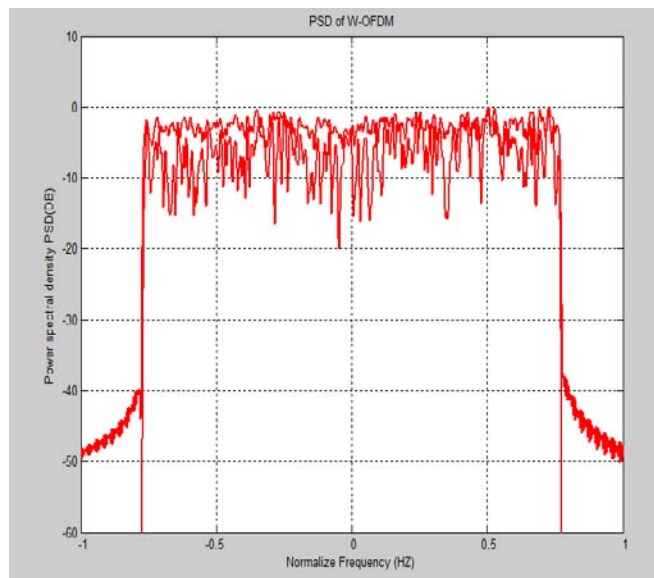



Figure 8: Power spectral density (PSD) of W-OFDM



PSD -60  
dB  
←

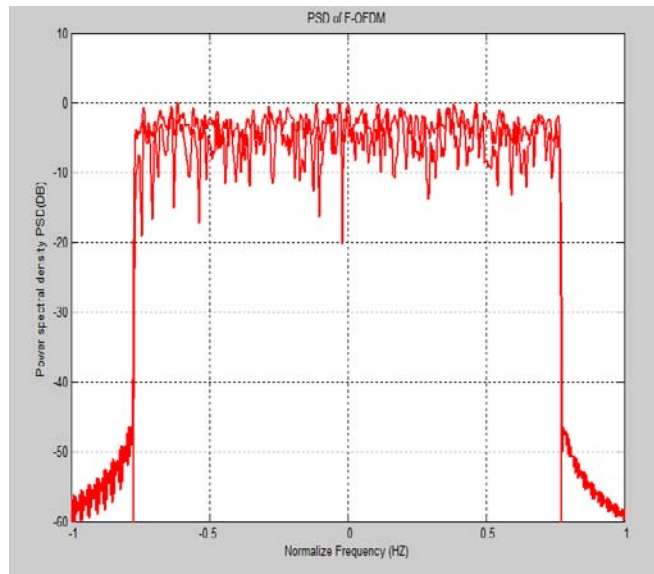


Figure 9: Power spectral density (PSD) of F-OFDM

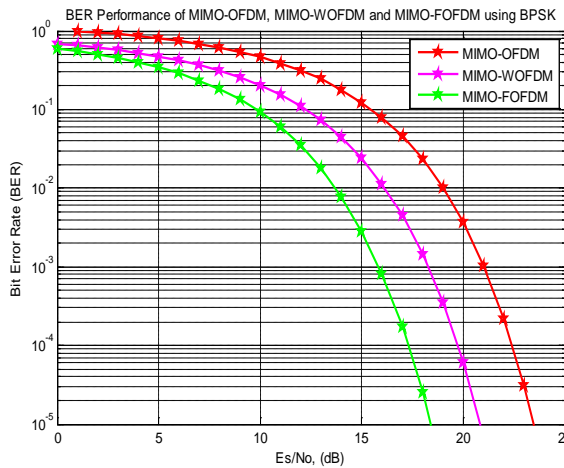


Figure 10: BER FOR MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh Fading Channel using BPSK

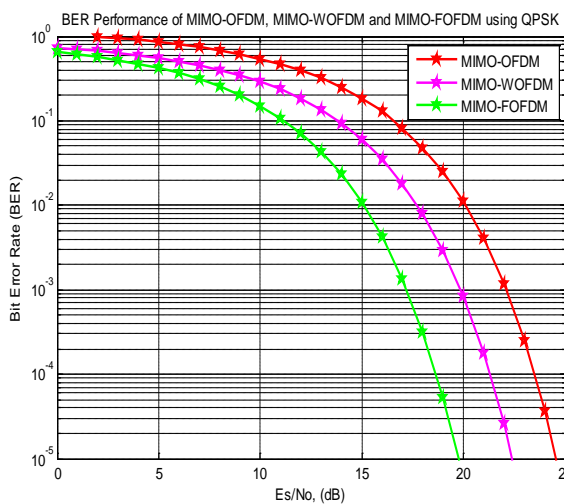


Figure 11: BER For MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh Fading Channel using QPSK

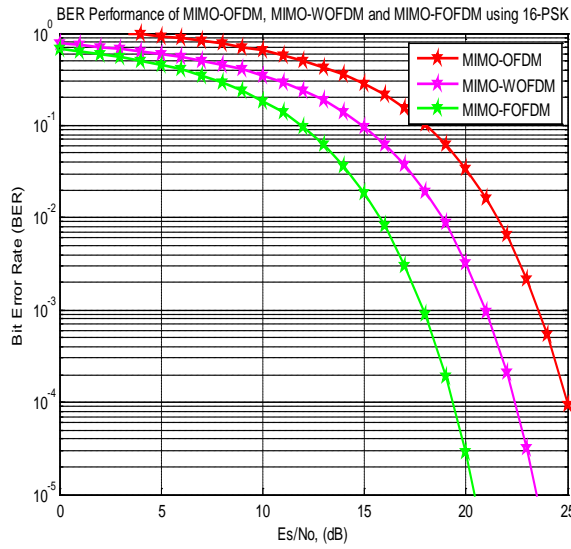


Figure 12: BER for MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh fading channel using 16-PSK

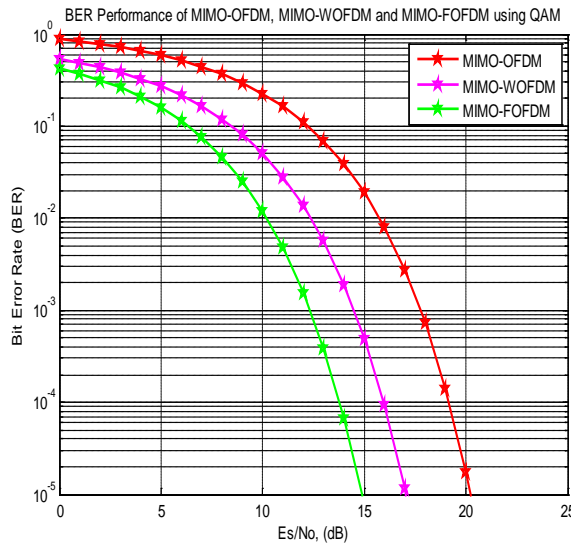


Figure 13: BER for MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh fading channel using QAM

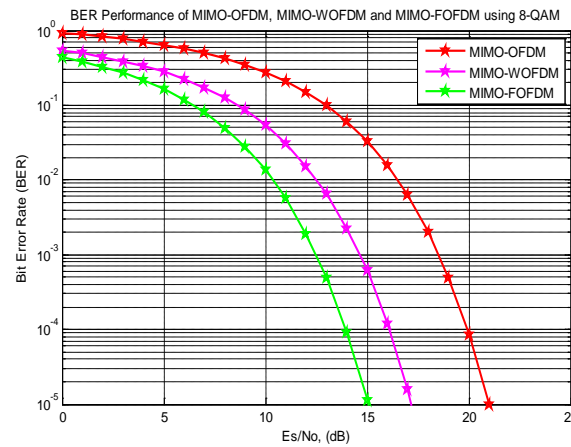


Figure 14: BER for MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh fading channel using 8-QAM.

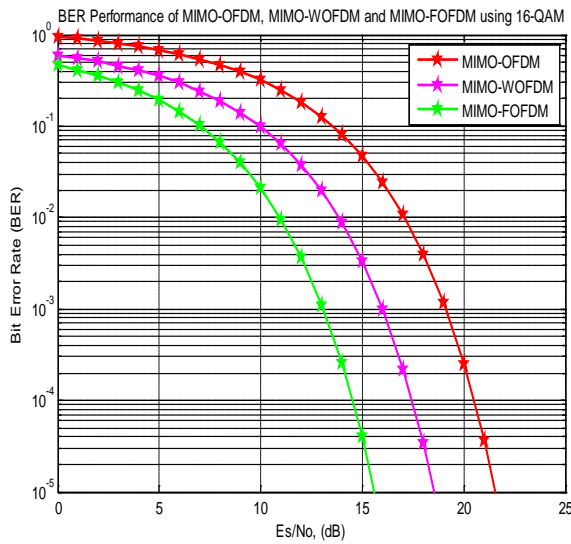


Figure 15: BER for MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM over Rayleigh fading channel using 16-QAM

Table 2: Data Table of Modulations, Multiplexing, Ber (Bit Error Rate) and Snr (Signal to Noise Ratio)

| Modulation | Multiplexing | BER       | SNR     |
|------------|--------------|-----------|---------|
| BPSK       | OFDM         | $10^{-5}$ | 23 dB   |
|            | W-OFDM       | $10^{-5}$ | 21 dB   |
|            | F-OFDM       | $10^{-5}$ | 18 dB   |
| QPSK       | OFDM         | $10^{-5}$ | 24 dB   |
|            | W-OFDM       | $10^{-5}$ | 23 dB   |
|            | F-OFDM       | $10^{-5}$ | 19.6 dB |
| 16-PSK     | OFDM         | $10^{-5}$ | 29 dB   |
|            | W-OFDM       | $10^{-5}$ | 24 dB   |
|            | F-OFDM       | $10^{-5}$ | 21 dB   |
| QAM        | OFDM         | $10^{-5}$ | 21 dB   |
|            | W-OFDM       | $10^{-5}$ | 17 dB   |
|            | F-OFDM       | $10^{-5}$ | 14.8 dB |
| 8-QAM      | OFDM         | $10^{-5}$ | 22 dB   |
|            | W-OFDM       | $10^{-5}$ | 17 dB   |
|            | F-OFDM       | $10^{-5}$ | 15 dB   |
| 16-QAM     | OFDM         | $10^{-5}$ | 22 dB   |
|            | W-OFDM       | $10^{-5}$ | 18 dB   |
|            | F-OFDM       | $10^{-5}$ | 16 dB   |

## VII. CONCLUSIONS

In this paper, the performance of MIMO-WOFDM system and its assessment with MIMO-OFDM, MIMO-WOFDM and MIMO-FOFDM systems by means of various modulations techniques is presented in this work. The SNR requirements for higher order PSK schemes are more to the acceptable range of BER over the simulated channel. It is also noteworthy that the higher orders of the QAM scheme have a little bit of significant influence over the performance of the both

simulated systems. Moreover, QAM requests lesser SNR as contrast to PSK for suitable BER for both the systems. To analyze BER, PSD and signal to noise ratio with BPSK, QPSK, 16-PSK, QAM, 8-QAM and 16-QAM modulation it can be concluded that among three multiplexers (OFDM, W-OFDM, and F-OFDM) F-OFDM provides high performance and bandwidth efficient in the wireless system.



## REFERENCES RÉFÉRENCES REFERENCIAS

1. P. Sudheesh, Jayakumar, A., Siddharth, R., Srikanth M. S., Bhaskar N. H., Dr. Sivakumar V., and Sudhakar C. K., "Cyclic prefix assisted sparse channel estimation for OFDM systems," in International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, 2012.
2. L. M. Rajeswari and Manocha, S. K., "Design of aata-adaptive IFFT/FFT block for OFDM system," in Proceedings - Annual IEEE India Conference: Engineering Sustainable Solutions, INDICON-2011.
3. F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski,
4. "Five disruptive technology directions for 5G," IEEE Communications Magazine, vol. 52, no. 2, pp. 74–80, 2014.
5. E. Hossain and M. Hasan, "5G cellular: key enabling technologies and research challenges," IEEE Instrumentation & Measurement Magazine, vol. 18, no. 3, pp. 11–21, 2015.
6. R. v. Nee and R. Prasad, "OFDM for wireless multimedia communications". Artech House, Inc., 2000.
7. X. Zhang, M. Jia, L. Chen, J. Ma, and J. Qiu, "Filtered-OFDM-enabler for flexible waveform in the 5th generation cellular networks," in Global Communications Conference (GLOBECOM). IEEE, 2015, pp. 1–6.
8. J. Abdoli, M. Jia, and J. Ma, "Filtered OFDM: A new waveform for future wireless systems," in Signal Processing Advances in Wireless Communications (SPAWC), 2015 IEEE 16th International Workshop on. IEEE, 2015, pp. 66–70.
9. Devika Rajeswaran and Aswathy K. Nair, "A novel approach for reduction of PAPR in OFDM communication," in Communication and Signal Processing (ICCSP), 2016 International. Conference on, IEEE, 2016.
10. K. Mizutani and H. Harada, "Universal Time-Domain Windowed OFDM," in Vehicular Technology Conference (VTC-Fall), 2016 IEEE 84th. IEEE, 2016, pp. 1–5.
11. Francesco Di Stasio, Marina Mondin, Fred Daneshgaran "Multirate 5G Downlink Performance Comparison for f-OFDM and w-OFDM Schemes with Different Numerologies," Marina Mondin is also affiliated with DET, Politecnico di Torino, C. so Duca degli Abruzzi 24, 10129, Torino, Italy (marina.mondin@polito.it).978-1-5386-3779-1/18/\$ 31.00 ©2018 IEEE.
12. L. Zhang, A. Ijaz, P. Xiao, M. Molu, and R. Tafazolli, "Filtered OFDM Systems, Algorithms and Performance Analysis for 5G and Beyond." in European Wireless 2018, 2018.
13. Y. Qiu, Z. Liu, and D. Qu, "Filtered bank based implementation for filtered OFDM," in 2017 7th IEEE Int. Conf. on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2017, pp. 15–18.
14. M. B. Mabrouk, M. Chafii, Y. Louet, and C. F. Bader, "A Precoding based PAPR Reduction Technique for UF-OFDM and Filtered-OFDM Modulations in 5G Systems," in European Wireless 2017, 2017.
15. D. Wu, X. Zhang, J. Qiu, L. Gu, Y. Saito, A. Benjebbour, and Y. Kishiyama, "A field trial of f-OFDM toward 5G," in Globecom Workshops (GC Wkshps), 2016 IEEE. IEEE, 2016, pp. 1–6.
16. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?," IEEE J. Select. Areas Commun., vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
17. Yojna Bellada, Shilpa Shrigiria, "Simulation and modeling of OFDM"
18. IEEE J. Select. Areas Commun., vol. 30, no. 3, pp. 100–108, Jun. 2014.
19. Systems and implementation on FPGA," in Proceedings of National Conference on Women in Science & Engineering (NCWSE 2013), SDMCET Dharwad.
20. P. Guan, D. Wu, T. Tian, J. Zhou, X. Zhang, L. Gu, A. Benjebbour, M. Iwabuchi, and Y. Kishiyama, "5G Field Trials: OFDM-Based Waveforms and Mixed Numerologies," IEEE Journal on Selected Areas in Communications, vol. 35, no. 6, pp. 1234–1243, 2017.
21. K. S. S. Michel C. Jeruchim, Philip Balaban, Simulation of Communication Systems: Modeling, Methodology and Techniques. Springer US, 2000. Fig. , vol. 30, no. 3, pp. 123–124, 2017.





This page is intentionally left blank



## A Secure Big Data Framework Based on Access Restriction and Preserved Level of Privacy

By Akinwunmi O. O, Onashoga S. A & Folorunso O.

*Federal University*

**Abstract-** Big data frequently contains huge amounts of personal identifiable information and therefore the protection of user's privacy becomes a challenge. Lots of researches had been administered on securing big data, but still limited in efficient privacy management and data sensitivity. This study designed a big data framework named Big Data-ARpM that is secured and enforces privacy and access restriction level. The internal components of Big Data-ARpM consists of six modules. Data Pre-processor which contains a data cleaning component that checks each entity of the data for conformity. Data Classifier deals with the classification of data due to the sensitivity of such data. Data Preservation consists of two sub modules with the goal of preserving data before release to any user or any third party application to prevent privacy violation of the data owner. Access Restriction module coordinates the user or third party application registration, access to data and information in the entire system.

**Keywords:** *differential privacy, big data, access restriction, data privacy.*

**GJCST-E Classification:** *D.4.6*



*Strictly as per the compliance and regulations of:*



# A Secure Big Data Framework Based on Access Restriction and Preserved Level of Privacy

Akinwunmi O. O<sup>α</sup>, Onashoga S. A<sup>σ</sup> & Folorunso O. P<sup>ρ</sup>

**Abstract-** Big data frequently contains huge amounts of personal identifiable information and therefore the protection of user's privacy becomes a challenge. Lots of researches had been administered on securing big data, but still limited in efficient privacy management and data sensitivity. This study designed a big data framework named Big Data-ARpM that is secured and enforces privacy and access restriction level. The internal components of Big Data-ARpM consists of six modules. Data Pre-processor which contains a data cleaning component that checks each entity of the data for conformity. Data Classifier deals with the classification of data due to the sensitivity of such data. Data Preservation consists of two sub modules with the goal of preserving data before release to any user or any third party application to prevent privacy violation of the data owner. Access Restriction module coordinates the user or third party application registration, access to data and information in the entire system. Parallel Processing and Distributed Storage handles all split processes in parallel across a cluster of servers and also stores and retrieves data across a distributed storage device. Request Management module handles all incoming requests from either application users and/or third party applications. Differential Privacy strategy acts on the solicitation by introducing a minimum distortion to the information provided by the database framework.

The distortion introduced is large enough as calculated by Laplace mechanism, to protect the privacy and at the same time small enough to enhance data utility. The Big Data-ARpM architecture is designed to run on a distributed server environment and to store and retrieve data from a parallel database system; this is because of the high velocity, volume and different varieties of data. Big Data-ARpM was implemented using the following tools: Python scripting and Java Programming languages, Mysql and Vm Ware on Apache Hadoop platform. To test the effectiveness of Big Data-ARpM, a medical dataset with 1,048,576 instances and 12 attributes was employed. Big Data-ARpM was evaluated based on its utility, scalability, accuracy, sensitivity, specificity and processing time. The results indicated accuracy of 95.80 %, sensitivity of 93.60 %, specificity of 98.00 % and 0.40 ms processing time with high utility and good scalability which shows that the time it takes to preserve a data of 5000 tuples or less are almost similar, as against K- Anonymity with respective values of 85.00 %, sensitivity of 80.00 %, specificity of 82.00 % and 0.45 ms with low utility and poor scalability. From these results, the appliance of differential privacy in

*Author α:* Department of Computer Science, D.S. Adegbenro ICT Polytechnic, Ewekoro, Ilori, Ogun State, Nigeria.

*e-mail:* akinwunmi.oluwafemi@dsadegbenropo ly.edu.ng

*Author σ ρ:* Department of Computer science, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria.

solving privacy issue proved a high level of efficiency. Hence, the deployment of a secure big data framework that is based on access restriction and preserved level of privacy posed a higher level of protection of user's privacy in comparison with other techniques.

**Keywords:** differential privacy, big data, access restriction, data privacy.

## I. INTRODUCTION

The developing wonder called big data is compelling various changes in organizations and different associations. Many battle just to deal with the gigantic informational collections and non-conventional information structures that are commonplace of big data.

Large information management is about two concepts: big data and data management, plus how the two work together to accomplish business and innovation objectives.

According to Ray (2018) Big Data refers to a large volume of diverse, complex and fast-changing data, derived from new data sources. The data sets are so large that is very difficult to manage by the traditional data processing software or the traditional software management (Manyika *et al.*, 2011; Gürsakal, 2014).

Big data is first about data volume, namely large datasets measured in tens of terabytes, or sometimes in hundreds of terabytes or petabytes. Also, big Data is so huge and complex that it is impossible for traditional systems and traditional data warehousing tools to process and work on them. Before the term enormous information became regular speech, we discussed Very Large Databases (VLDBs). VLDBs usually contain exclusively structured data, managed in a database management system (DBMS).

Notwithstanding exceptionally huge datasets, large information can likewise be a mixed blend of organized information (social information), unstructured information (human language content), semi-organized information (RFID, XML), and spilling information (from machines, sensors, Web applications, and web-based social networking). The term multi-organized information alludes to informational collections or information conditions that incorporate a blend of these information types and structures. (Gantz and Reinsel, 2011).

With the expansion in the utilization of big data in business, numerous organizations are grappling with privacy issues. Information protection is a risk, consequently organizations must be on security cautious. Security is the case of people, gatherings, or organizations to decide for themselves when, how, and to what degree data about them is imparted to other people. In contrast to security, privacy ought to be considered as a benefit; in this manner it turns into a selling point for the two clients and different partners. There ought to be a harmony between data privacy and national security.

## II. RELATED WORK

Lu et al., (2014) made a methodology towards the proficient and protection saving processing in the big data period, and it misuses the new difficulties of big data in security safeguarding. At first, it characterizes the general engineering of big data examination and finds the security necessities in big data. At that point, it discovers a proficient and privacy preserving cosine closeness figuring convention. The limitation of the work is that it needs significant research efforts for addressing unique privacy issues in some specific big data analytics.

Xu et al., (2016) structured a system named "Rampart framework" for privacy safeguarding. It comprises of techniques in particular anonymization, recreation, change, provenance, understanding, exchange and limitation to forestall outside interruption. The system endeavored to give high need to keep up the harmony between information utility and privacy however recommended that more ways are to be investigated to ensure protection against different dangers.

Shrivastva et al., (2014) broke down how much the differential privacy approach is appropriate for big data security conservation and introduced different elements that assume key job in big data security safeguarding. Among the different methodologies, differential privacy is the best appropriate for big data as it is liberated from the imperfections of different methodologies. Plus, differential privacy looks for balance among utility and security. A framework of perturbation is introduced to accomplish the differential privacy.

Al-Aqeeli and Alinfie (2015) researched some security saving issues of big data with regards to half breed distributed computing and assessed a few systems, for example, Airavat, Sedic, Sac FRAPP and Hyper-1 dependent on Map Reduce from the point of view of versatility, cost and similarity. It was recorded that anonymization, encryption, differential privacy are the productive strategies for ensuring protection of information. The last investigation shows that the featured structures experiences constraints, for

example, information contortion and none of them is completely fit for privacy preservation.

Mehmood et al., (2016) introduced existing protection safeguarding instruments in the different life patterns of big data, for example, data generation (encryption and access limitations), information stockpiling (hybrid and private mists) and information handling (generalization, suppression, anatomization, permutation and perturbation) and different difficulties of saving security in large information. These techniques were portrayed as for the variables of versatility, security, time, proficiency and utility. Different dangers engaged with the encryption, anonymization and capacity of information in the cloud were likewise researched. At the point when these strategies are applied, security is ensured however the information may lose the importance in reality and thus the utility and criticalness. For information distributing, a calculation must consider legitimate exchange off among utility and security as the information is inclined to any assaults. Along these lines the strategies/methods must be adjusted or stretched out to deal with the large information in a proficient way.

Yan et al., (2016) proposed a pragmatic plan to deal with the encoded big data in cloud with de duplication dependent on possession challenge and Proxy Re-Encryption (PRE). As recognized by Jian et al., (2016), the constraint of their work is that Convergent Encryption (CE) is dependent upon an innate security restriction for example powerlessness to disconnected animal power word reference assault.

Sedayao et al., (2014) introduced a contextual investigation of anonymization in an endeavor identifying the necessities and execution detail for saving security of enormous information. Anonymized informational collections must be painstakingly broke down, estimated and tried whether they are inclined to any assaults since it is more than covering or generalization. The creators recommended the utilization of Hadoop to break down and get helpful outcomes from the big data. The analyses are led with static informational index, yet it ought to be stretched out for continuous informational indexes. The work couldn't reason that the anonymized information is completely liberated from any sort of assaults.

Zakerdah and Aggarwal (2015) proposed a methodology towards protection safeguarding information mining of exceptionally monstrous informational indexes utilizing map reduce. They study two most broadly utilized security models k-anonymity and l-diversity variety for anonymization, and present test results outlining the effectiveness of the methodology. The constraint of their work is that generalization cannot deal with high dimensional information, it decreases information utility. Perturbation decreases utility of information.

Zhang et al., (2013) proposed Cloud Safe to redesign availability and mystery of the set aside



information in the cloud through scrambling and encoding data into a couple of disseminated stockpiling providers. Cloud Safe offers a cloud-based individual electronic asset safe help which passes on the critical assets between a couple of cloud providers by using destruction coding and cryptography. As per Zhang et al., (2013), the accessibility improves because of utilizing eradication coding to disperse the information on a few cloud suppliers, so as to recoup information get to when a supplier falls flat. AES was utilized for scrambling and unscrambling information to keep information secrecy.

Zhang et al., (2014) researched the versatility issue of multidimensional anonymization over big data on cloud, and proposed an adaptable Map Reduce based methodology. The flexibility issues of finding the center on account of its inside activity in multidimensional allotting was investigated and significantly versatile Map Reduce based computation was proposed for finding the center and histogram strategy. Logically number of investigations on datasets were coordinated which was removed from real datasets, and the exploratory results show that the flexibility and cost sufficiency of multidimensional anonymization plan can be improved basically over existing techniques, anyway ensuring insurance protecting of immense extension educational assortments regardless of everything needs wide assessment.

Pramanik et al., (2016) presented a conceptual framework that integrates and improves technologies for preserving big data privacy. The proposed model

empowers the structure of a dependable protection framework for a given e-government procedure and comprises of three significant modules: a) Big information assortment, b) Information extraction, and c) Anonymization module. In this work, a Conditional Random Field (CRF) classifier was conveyed for extricating distinguishing characteristics, and k-anonymization strategy for de-recognizing the separated information through insignificant speculation and concealment. The creators likewise introduced a lot of primer trial results indicating the viability of the proposed structure dependent on some security assessment measurements.

### III. DESIGN METHODOLOGY

The architecture named Big Data-ARpM (Big Data Access Restriction and Privacy Mechanism) is defined by the collection or gathering of data with high velocity, volume and different varieties, classification of the gathered data, storing the data securely and restricting the access to data from within and out of the systems. Figure 1a is a physical architecture that gives an insight into the operational structure of Big Data-ARpM, Figure 1b shows the internal structures of the Access Restriction and the Key Management Module, while Figure 1c shows the internal structure of the request management module. The architecture is designed to run on a distributed server environment and to store and retrieve data from a parallel database system; this is because of the high velocity, volume and different varieties of data.

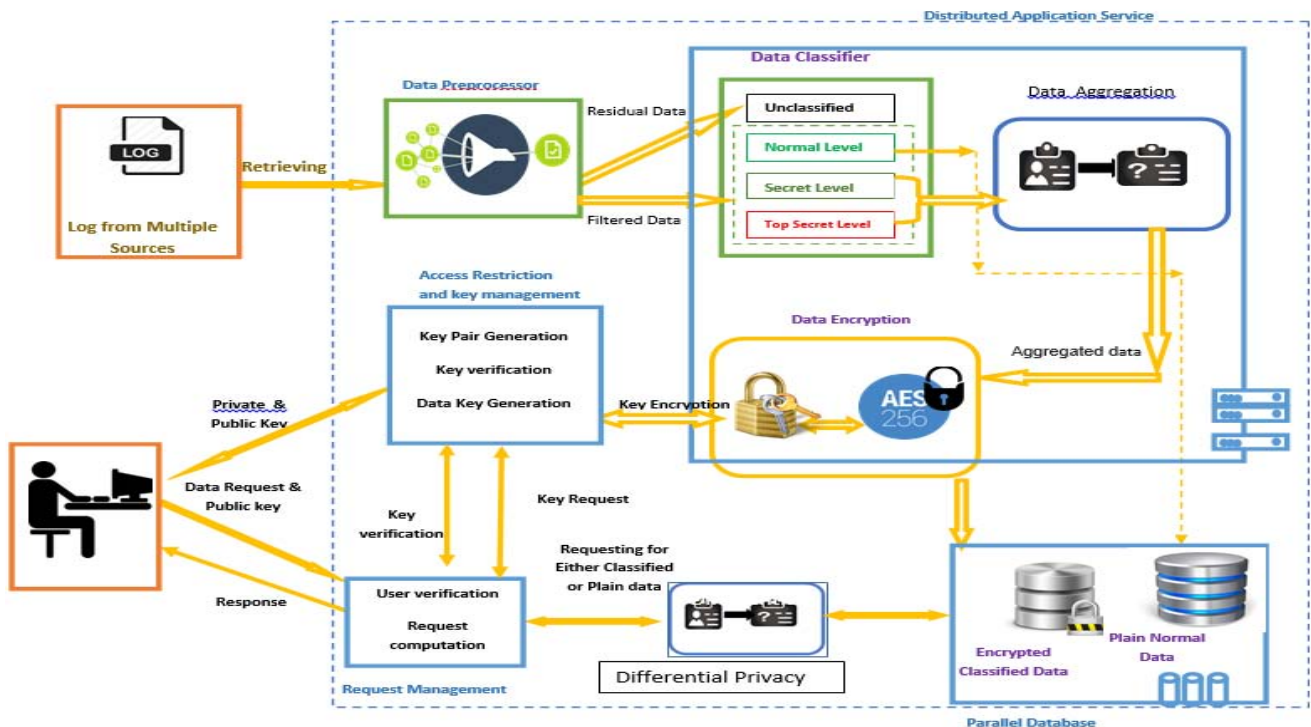


Figure 1a: Big Data-ARpM framework

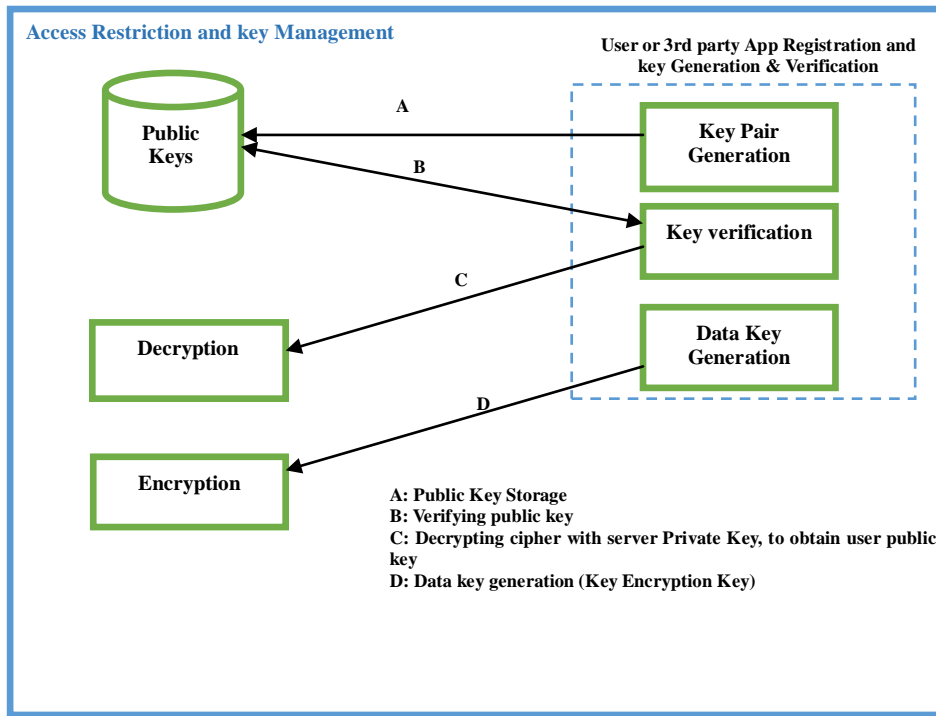


Figure 1b: Access Restriction and the Key Management Module.

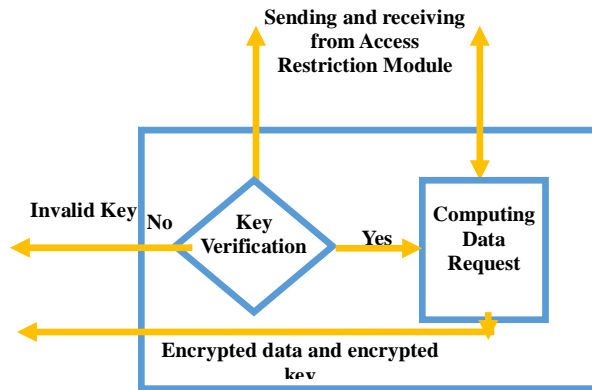


Figure 1c: Request Management Module

a) *Internal Components of Big Data-ARpM*

Big Data-Arp Mretrieves input from synchronous multiple data sources, these input are raw and however need to be pre-processed and further classified before its then stored securely and await a request for delivery, because the data may contain sensitive information of so many entities, people and organization, releasing the data without anonymizing them may be a very great disaster, Big Data-Arp Mhas a well-structured internal component that facilitates all the processes, the structures and their respective functions are;

**ALGORITHM 1: Preprocessor Algorithm**

```

Procedure Preprocessor (Record D){
//column screen
While (D hasvalue){ // loop through each field of D
If(!isValidField(Di)){ //check if each filed is not empty or is a valid data

```

b) *Data Pre-processor Module*

Data pre-processing is an important step in data gathering, data gathering are mostly loosely controlled, resulting in out of range value (Age: -100) and impossible data combinations e.g. (Sex: Male, Pregnant: Yes). Data that are being gathered and input from the source (WebCrawler) are considered to be noisy-data, however the Data Pre-Processor Module contain a data cleaning component that check each entity of the data for conformity, the output from the data pre-process is a processed and filtered data.

```

Return false
}
}
// structure screen
If(D.lenght<ExpectedFieldSize){
 Return false
}
While (D hasFiled){ // loop through each field Title of D
If(!ValidField(DT;)){ // check if the field is among expected filed
Return false
}
}
Return true
}

```

#### IV. DATA CLASSIFICATION MODULE

This module deals with the classification of data due to the sensitivity of such data. The role assigned to the user will determine what class of data such data users can access. There are three basic levels of classifications in this module, which are:

- *Normal Level:* Users assigned to this level can only view attributes such as the Quasi-identifier (QID). (QID) is a set of attributes such as zip code, gender, a birth date in which the combination of this attributes could potentially distinguish individuals. This level is the least sensitive of all the three levels.
- *Secret Level:* This level deals with attributes that are considered to be explicit identifiers. Explicit Identifier is a set of attributes that contains information that can be used to identify individuals such as name, security number uniquely. This level is more sensitive than the normal level. Users assigned to this level can view both the normal and secret level.
- *Top Secret Level:* This is the most sensitive level of the three levels. Users under this level are given access to view all the three levels. Attributes under this level are considered to be Sensitive identifier. Sensitive attributes contain sensitive personal information such as medical history, salary.

*ALGORITHM 2: Data Classification Algorithm*

Input: *document-data, dd.*

Output: *list of <attribute, value>*

*Begin*

*Step 1: Frequently pull data through API*

*Step 2: process Filter (dd);*

*Step 3: retrieve Privacy Level (); // Normal Level, Secret Level, Top Secret Level*

*Step 4: data Classifier (process Filter, retrieve Privacy Level());*

*Step 5: update Database (data Classifier);*

*Step 6: validate Data (retrieve Privacy Level, update Database);*

*Step 7: List useful attribute-value data from the document-data.*

*End*

#### V. DATA PRESERVATION MODULE

The Module consist of two sub modules with the goal of preserving data before release to any user or any third party application to prevent the privacy violation of the data owner. The data passes through the first module that build an aggregated tree of a single sink data from various data coming from various sources of data entries; this reduces the chances of tracing back the data back to the original owner , prim's algorithm was employed to build the tree. The aggregated data is then passed on to the differential privacy module, which introduce a minimum distortion in the information provided by the database system.

*ALGORITHM 3: Differential Privacy Algorithm*

Input: *Level, dp Request*

Output: *DP\_response*

*Begin*

*Step 1: The analyst can make query to the database through this intermediary privacy guard.*

*Step 2: The privacy guard takes the query from the analyst and evaluate this query and other earlier queries for the privacy risk. After evaluation of the privacy risk.*

*Step 3: The privacy guard then gets the answer from the database*

*Step 4: Add some distortion to it according to the evaluated privacy risk and finally provide it to the analyst.*

*End*

##### a) Access Restriction and Key Management module

This modules consists of different sub modules, that coordinates the user or third party application registration, access to data and information in the entire systems, the modules are

- Key Generation module
- Key verification module
- Data key generation module

All the modules rely on the RSA public key crypto system for the following

- RSA Encryption
- RSA Decryption

- RSA Key Generation
- RSA Signing and
- RSA Verifications

b) *Parallel Processing and Distributed Storage module*

Due to high velocity and large volume of data that will be passing through the system, this module is designed to handle all split processes in parallel across a cluster of servers and also store and retrieve data across a distributed storage devices, the modules uses Map Reduce, which is programming model for processing large set of data with a parallel and distributed algorithm across a cluster of server.

c) *Request Management Module*

The module handles all incoming request from either application users and or third party applications with the aid of the access restriction module which verify the membership of the users, and also analyse the request to know the level of information been requested, check if the level of the user can access the level of information requested. After the user successful verification, the users query/ request passes through differential privacy technique which deny the users direct access to the database.

ALGORITHM 9: Request Management Algorithm

Input: *Incoming request.*

Output: *Preserved outgoing data*

*Begin*

*Step 1: Login credentials validated by access restriction module → True/False*

*Step 2: If “True”, request interface is displayed. Access Granted.*

*Otherwise, the user is an unauthorized user. Access Denied.*

*Step 3: If “Access Granted” Then Level ← call Request User Level();*

*Send Request (req, level, res);*

*dp ← DP(res,level);*

*Step 4: Is True (dp): process Result (dp→result): preserved Data (dp→result);*

*Step 5: Output Request (dp→result);*

*Step 6: otherwise, goto step 3.*

*End*

VI. DATA SET

A medical dataset was used in the implementation of Big Data-ARpM, the dataset, named Health Care Provider Credential Data was downloaded from an open source called “data.wa.gov”. The dataset contains more than a million instances (records) and 12 attributes (Columns).

VII. RESULTS AND DISCUSSIONS

Table 1: Comparing Differential Privacy (DP) and K-Anonymity

| Evaluation Metrics | Differential Privacy (DP) | K-Anonymity |
|--------------------|---------------------------|-------------|
| Data Utility       | High                      | Low         |
| Scalability        | Good                      | Poor        |
| Accuracy           | 95.80%                    | 85.00%      |
| Sensitivity        | 93.60%                    | 80.00%      |
| Specificity        | 98.00%                    | 82.00%      |
| Processing Time    | 0.40 ms                   | 0.45 ms     |

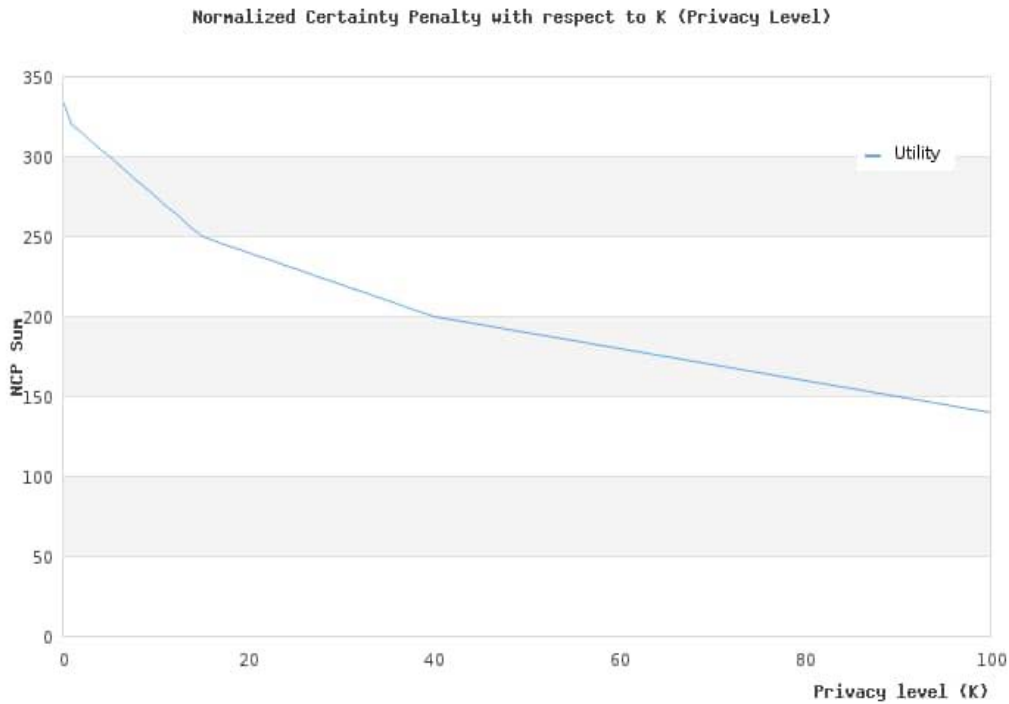


Figure 2: Normalized Certainty Penalty with respect to K (Privacy Level)

Figure 2 depicts the summation of normalized range of equivalence classes with high privacy (low value of k) having the higher normalized certainty penalty than those with low privacy. Even though, the normalized range of each equivalence classes in high

privacy is small, the number of tuples in each equivalence group are high that their summation is larger than the normalized range of equivalence classes in lower privacy (high value of K).

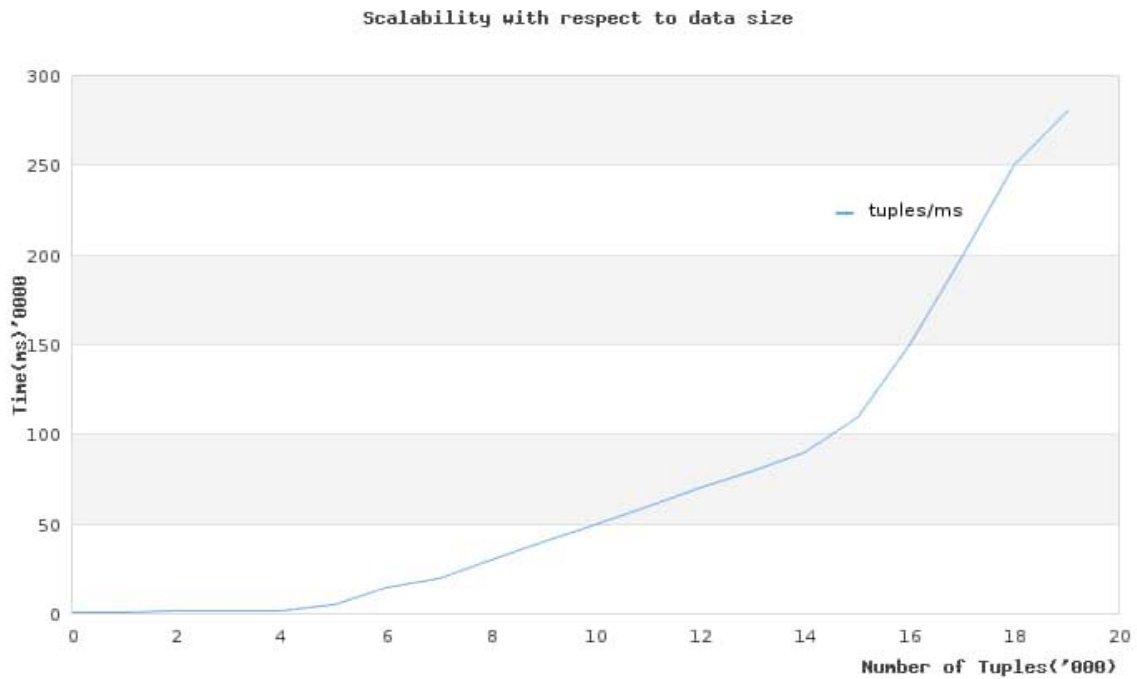


Figure 3: Scalability with respect to the database size

Figure 3 depicts that the scalability of the system with the data size to be anonymized. The result shows that the time it takes to preserve a dataset of 5000 tuples or less tuples are almost similar, but as the

dataset gets bigger the time it takes to complete the preservation increases steadily. Thus, our preservation input dataset will have a strong effect on the performance of preservation.



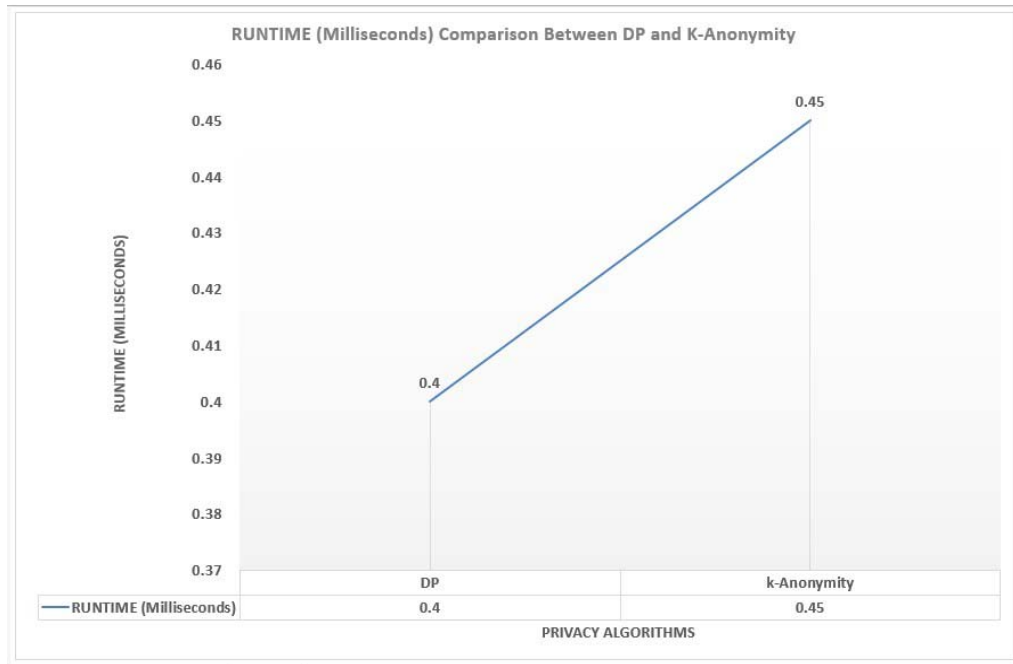


Figure 4: Runtime comparisons between DP and k-Anonymity privacy algorithms

The computation time is measured in milliseconds and on Big Data platform, the comparisons depict that DP takes lesser computational time in protecting data privacy against k-Anonymity to complete protecting data privacy with 0.4 and 0.45 milliseconds

values respectively. This shows that DP is quiet better when privacy protection of data is needed and processing time is to be considered in Big Data analytics.

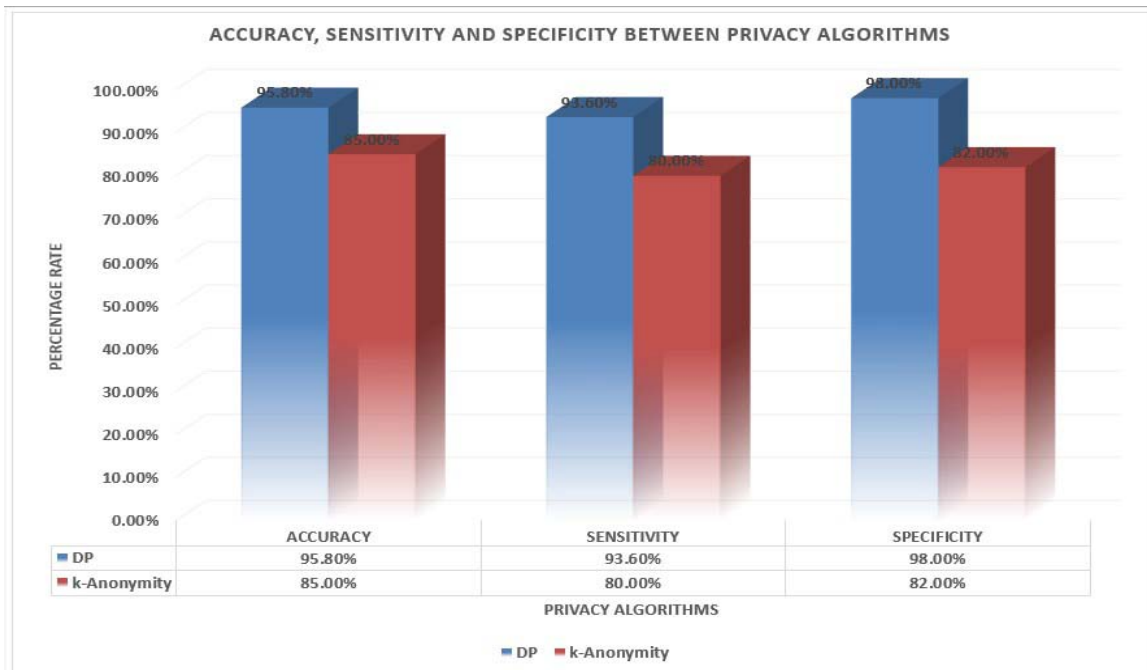


Figure 5: Comparisons between privacy algorithms in terms of accuracy, sensitivity and specificity

The figure 5 illustrate that DP is best for applying on data privacy issues as against k-Anonymity and others as regards accuracy, sensitivity and specificity with 95.80%, 93.60%, 98.00% and 85.00,

80.00, 82.00% values respectively. Though, k-Anonymity is closer to DP in this comparison but we have DP to protect privacy better than it does.

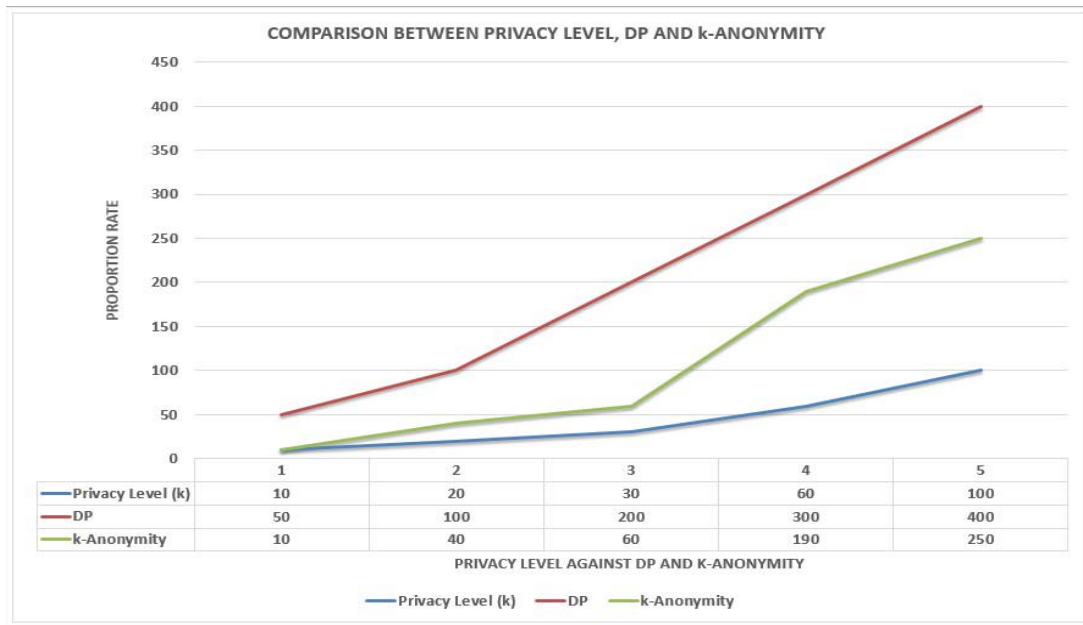


Figure 6: The comparison between Big Data privacy algorithms with respect to privacy level

This illustrates that DP produced more records that is useful for analyst with an increase in privacy level while as the privacy level (k) increased, k-Anonymity produced few records with the utility lesser than DP. For instance, when the privacy level applied is 20 and 60, DP present a total of 100 and 300 records against 40 and 190 records produced by k-Anonymity which shows

that as the level of privacy level in DP generate more useful records that can be used for analysis while the confidentiality of data are hiding. Though, DP and k-Anonymity have the same privacy level (k), the utility of records generated from each algorithm differs and depict that DP produced more useful data than k-Anonymity.

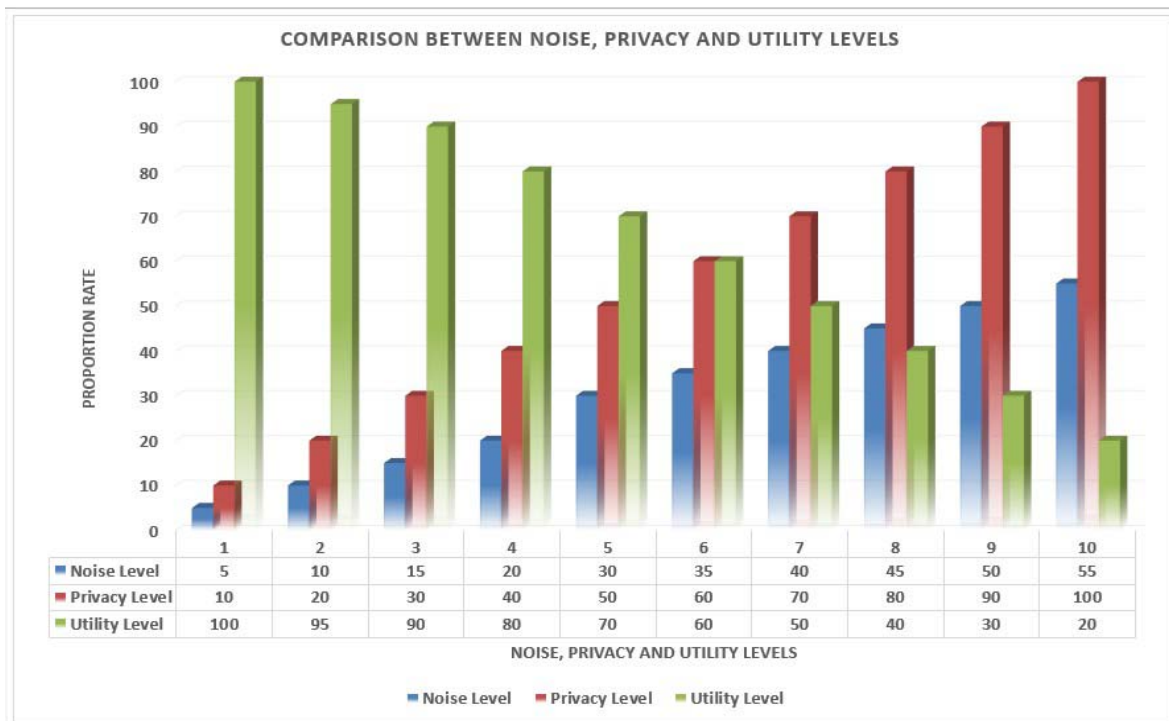


Figure 7: Comparison between the noise, privacy and utility levels

In this paper, the approach DP used applied noise variant in achieving its purpose as depicted in Figure 7 showing the comparison between the noise, privacy and utility levels. The privacy level shows the protection of data from being identified, the utility level shows the usefulness of data after noise has been added to user's queries and noise level is privacy balanced added to individual record based on the attribute of each data and the level of each user requesting for data. For example, when the noise level is 10, privacy and utility level are 20 and 95 values respectively revealing that the more noise added, there is increase in the privacy and decrease in the utility of data information presented to the users. This also shows that, there is every possibility that we have the same level of privacy and utility of data as shown where we have noise level to be 35 added, privacy and utility levels having 60 respectively and this means that DP +Noise give rise to privacy preserving of data with a reasonable amount of utility than k-Anonymity algorithm.

## VIII. CONCLUSION

In this study, a conceptual privacy and access restricted framework for securing big data was conceived by designing a data classification scheme according to degree of confidentiality and also designing a privacy preservation technique that enforces data privacy based on data aggregation and differential privacy.

Conclusively, Big Data-ARpM was evaluated based on its utility, scalability, accuracy, sensitivity, specificity and processing time. The results shows that Big Data-ARpM has a very good utility, highly scalable, accuracy of 95.80%, sensitivity of 93.60%, specificity of 98.00% and an execution time of 0.4 milliseconds, as compared with other privacy preservation techniques such as K-anonymity. Hence, the usage of differential privacy technique in Big Data ARpM show that the framework is far better than other frameworks that makes use of other technique.

## IX. RECOMMENDATION

With the efficient techniques presented in this research work, it is believed that the study can be easily extended to focus more on other type of data such as the semi-structured data and unstructured data. Finally, the presented framework can be built upon to accept larger files of different formats.

## REFERENCES RÉFÉRENCES REFERENCIAS

- Al-Aqeeli, S., and Alnifie, G. 2015. Preserving Privacy in Map Reduce Based Clouds: Insight into Frameworks and Approaches. *International Conference on Cloud Computing (ICCC)*. doi:10.1109/cloudcomp.2015.7149652.
- Gantz, J. and Reinsel, D. 2011. Extracting value from chaos. IDC iView, (1142), 9-10.
- Gartner 2014. IT Glossary, What is Big Data? URL: <http://www.gartner.com/it-glossary/big-data/>, (Son Erişim Tarihi: 20.12.2014).
- Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., and Khan, S. U. 2015. The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*47: 98-115.
- Lu, R., Zhu, H., Liu, X., Liu, J. K., & Shao, J. (2014). Toward efficient and privacy-preserving computing in big data era. *IEEE Network*, 28(4), pp. 46-50. <https://doi.org/10.1109/MNET.2014.6863131>.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. and Byers, A.H. 2011. Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey Global Institute, Seattle, May 2011.
- Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. 2016 Protection of big data privacy. In: IEEE translations and content mining are permitted for academic research, pp 245-256.
- Pramanik, MdIleas; Lau, Raymond Y. K.; and Yue, Wei T., 2016. "A Privacy Preserving Framework for Big Data in E-Government". *PACIS 2016 Proceedings*. 72. <https://aisel.aisnet.org/pacis2016/72>.
- Ray R, 2018. The-complete-beginners-guide-to-big-data-in-2018. <https://medium.com/swlh/the-complete-beginners-guide-to-big-data-in-201882ed7a396ba3>
- Sedayao, J., Bhardwaj, R., and Gorade, N. 2014. Making Big Data, Privacy, and Anonymization Work Together in the Enterprise: Experiences and Issues. *IEEE International Congress on Big Data*. doi:10.1109/bigdata.congress.2014.92.
- Shrivastva, K. M., Rizvi, M. and Singh, S. 2014. Big Data Privacy Based on Differential Privacy Hope for Big Data. *International Conference on Computational Intelligence and Communication Networks*. Pp.167.
- Xu, L., Jiang, C., Chen, Y., Wang, J., and Ren, Y. 2016. A Framework for Categorizing and Applying Privacy Preservation Techniques in Big Data Mining. *Computer*, 49(2):54-62.
- Yan Z, Ding W, Xixun Yu, Zhu H, and Deng RH. 2016. Deduplication on encrypted big data in cloud. *IEEE Trans Big Data*; 2(2):38-50.
- Zakerdah H C. C, and Aggarwal KB. 2015 Privacy-preserving big data publishing. La Jolla: ACM. Zhang Q, Luo B, Shi W, Almoharib AM. Cloud Safe: Storing Your Digital Asset in the Cloud-based Safe. Wayne State University. Pp 243-251.
- Zhang Q, Luo B, Shi W, Almoharib AM. 2013. CloudSafe: Storing Your Digital Asset in the Cloud-based Safe. Wayne State University. Pp 243-251.

16. Zhang X, Yang T, Liu C, Chen J. 2014. A scalable two-phase top-down specialization approach for data Anonymization using systems, in Map Reduce on cloud. *IEEE Trans Parallel Distrib* 25(2): 363–73.





This page is intentionally left blank





## No Fish; Total Anti-Phishing Protection System

By Dhanushka Niroshan Atimorathanna, Tharindu Shehan Ranaweera,  
R A H Devdunie Pabasara, Jayani Rukshila Perera  
& Kavinga Yapa Abeywardena

**Abstract-** Phishing attacks have been identified by researchers as one of the major cyber-attack vectors which the general public has to face today. Although software companies launch new anti-phishing products, these products cannot prevent all the phishing attacks. The proposed solution, “No Fish” is a total anti-phishing protection system created especially for end-users as well as for organizations. In this paper, a realtime anti-phishing system, which has been implemented using four main phishing detection mechanisms, is proposed. The system has the following distinguishing properties from related studies in the literature: language independence, use of a considerable amount of phishing and legitimate data, real-time execution, detection of new websites, detecting zero-hour phishing attacks and use of feature-rich classifiers, visual image comparison, DNS phishing detection, email client plug in and specially the overall system has designed to the levelbased security architecture to reduce the time-consumption.

**Keywords:** *cyber-attack, anti-phishing, information security, machine learning, visual similarity, feature extraction, natural language processing.*

**GJCST-E Classification:** D.4.6



NOFISHTOTALANTI-PHISHINGPROTECTIONSYSTEM

*Strictly as per the compliance and regulations of:*



RESEARCH | DIVERSITY | ETHICS

# No Fish; Total Anti-Phishing Protection System

Dhanushka Niroshan Atimorathanna <sup>α</sup>, Tharindu Shehan Ranaweera <sup>σ</sup>, R A H Devdunie Pabasara <sup>ρ</sup>,  
Jayani Rukshila Perera <sup>ω</sup> & Kavinga Yapa Abeywardena <sup>¥</sup>

**Abstract** Phishing attacks have been identified by researchers as one of the major cyber-attack vectors which the general public has to face today. Although software companies launch new anti-phishing products, these products cannot prevent all the phishing attacks. The proposed solution, “No Fish” is a total anti-phishing protection system created especially for end-users as well as for organizations. In this paper, a real-time anti-phishing system, which has been implemented using four main phishing detection mechanisms, is proposed. The system has the following distinguishing properties from related studies in the literature: language independence, use of a considerable amount of phishing and legitimate data, real-time execution, detection of new websites, detecting zero-hour phishing attacks and use of feature-rich classifiers, visual image comparison, DNS phishing detection, email client plug in and specially the overall system has designed to the level-based security architecture to reduce the time-consumption. Users can simply download No Fish browser extension and email plug in and protect themselves, establishing a relatively secure browsing environment.

**Keywords:** cyber-attack, anti-phishing, information security, machine learning, visual similarity, feature extraction, natural language processing.

## I. INTRODUCTION

Nowadays, with advances in technology, internet-related crimes have increased at an alarming rate [1]. Among these crimes, phishing is one of the most popular cyber-attack vectors, which is a serious threat to information security and especially to the global economy. In phishing attacks, attacker develops web pages mimicking original websites and sends out fake emails, impersonating as a trusted entity such as popular brands or organizations, asking for sensitive information such as username, password, phone number, credit card details and other personal information. Internet users should be aware of phishing attacks as it has been in the cyber domain for years. However, many people still tend to fall victim and leak confidential information through suspicious web pages.

There are common ways of fighting phishing attacks. One way is to train employees to recognize the gravity of phishing attacks and their consequences. Awareness plays a crucial role in phishing prevention [2]. However, it is not practical to train employees or

*Author <sup>α σ ρ ¥</sup>:* Dept. of Computer Systems Engineering Sri Lanka Institute of Information Technology Malabe, Sri Lanka.

*e-mails:* kavinga.y@sliit.lk, dhniroshan@gmail.com, tharinduranaweera94@gmail.com, devdunie.r@gmail.com

*Author <sup>ω</sup>:* Dept. of Software Engineering Sri Lanka Institute of Information Technology Malabe, Sri Lanka.

*e-mail:* rukjayani@gmail.com

users on every possible phishing scenario. It is only human nature to be distracted and deceived. The other way is to block domain URLs and IPs, which are known from previous phishing attacks. However, hackers constantly create new domains to hunt fresh IPs [3]. The proposed “NoFish” identifies the website which the user is about to visit. It identifies logos and important features of a website using machine learning to detect the website which is being visited by the user. The visual similarity between the legitimate website and the current website is compared to get more accurate results. “NoFish” has an email client plugin for the Microsoft Outlook email client, which is implemented using content-based approaches and client-based programming languages. It should be downloaded to the Microsoft Outlook email client and it detects spam emails and extract URLs from the email body for further analysis. “NoFish” uses different classification algorithms, machine learning (ML), and natural language processing (NLP) based features [4]. NLP is proposed for URL analysis. It detects phishing URLs that users are about to visit. When using untrusted internet connections such as public WiFi services, DNS based anti-phishing approach, and HTTPS certificate transparency checking system are used to protect against DNS related phishing attacks [5][6]. The system provides a feedback mechanism to enhance user experience through a dashboard. ‘NoFish’ innovative solution detects all kinds of phishing attacks, including future ones after a super simple deployment next to the user’s email client and web browser. It implements a simple email client plug in and browser extension for users.

## II. RELATED WORK

Phishing is a major security issue that needs to be addressed. Internet users should be aware of phishing attacks because this has been around for years. However, many domestic users still tend to get tricked by these phishing attempts. Therefore, everyone needed a good software-based solution to overcome this human error. In recent years, industry and academia have proposed several anti-phishing solutions to counter the phishing threat. Some of the important methods are discussed below.

### a) Document Object Format

Document Object Format (DOM) is a language-independent and cross-platform programming interface

for XML, XHTML, and HTML documents [7]. The DOM is an object-oriented representation of the web page. The DOM-based phishing detection solutions use the similarity of a DOM tree on a suspicious web page and a legitimate web page to detect phishing. Since attackers always imitate a legitimate web page and create phishing web pages, the layout of the page is expected to be the same. Rosiello et al. have proposed a solution that alerts users when they use the same information on different websites, such as the same username and password [7].

#### b) Content-based comparison

Content-based comparison often attempts to compare the text of a web page through machine learning. Using the TF-IDF, the most used algorithm for extracting text and information from the web page, al. Zhang developed a content-based system to identify phishing websites [8]. Basnett et al. Evaluate their performance using various machine learning techniques, including neural networks, SVM (Support Vector Machine), and SOM (Self-Organizing feature Map) [8] [9].

#### c) Signature-based technique

Huang proposed a unique signature-based method to identify legitimate websites using text keywords and images on the website [10]. The system compares the signature of the currently open website with the signature database when a user tries to log in to a new website. If the domain name is changed but the signature matches, the web page will be declared as phishing. When a user visits a website for the first time, the system generates the signature and saves it to the database. Therefore this detection only works for the previously visited website sites, and it cannot detect zero-hour phishing attacks.

#### d) Phish Zoo

Afros and Greens tad have proposed a phishing detection solution called "Phish Zoo" that creates a unique profile for a website using URL, images, text content, secure connection layer (SSL) certification, and script [11]. When a user visits a website, Phish Zoo matches the current site profile with a list of legitimate sites and profiles stored in the database. As a first step, the URL and SSL certificate is compared with the stored profile. If it matches, the website is considered legitimate by Phish Zoo. Otherwise, the site's contents will be matched against appearance profiles to detect phishing attempts.

uses a level-based detection mechanism to identify phishing attacks in order to reduce the computational power and time consumption. Therefore it increases the performance and accuracy of the overall product than existing systems. Further, it provides protection against phishing attacks on trusted and untrusted internet connection. If the user is using an untrusted internet connection such as public WiFi, then the system checks the trustworthiness of the DNS servers [5] [12][13]. Otherwise, it will be forwarded to the usual phishing detection mechanism. The system architecture is proposed under six main components. They are namely:

- Browser Extension
- URL Analysis
- Image Processing
- Email Phishing Detection
- DNS Phishing
- Feedback Mechanism

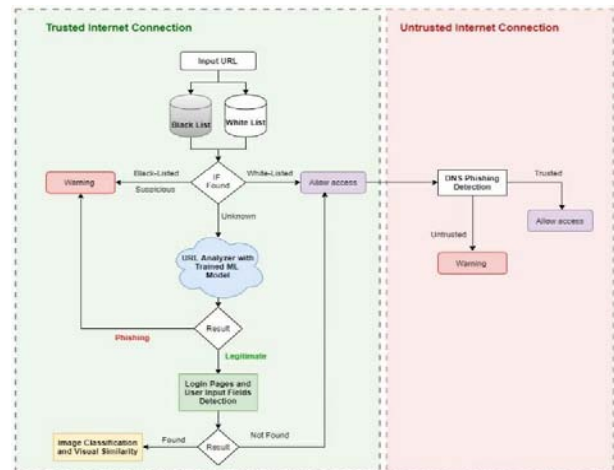


Figure 1: Overall Flow Chart of NoFish

NoFish uses a level-based security mechanism to detect phishing attacks. Researches have designed it in such a manner to reduce the computational power, reduce the time consumption of the NoFish clients, and to increase the performance and accuracy of the overall product. Figure 1 depicts the flow chart of the proposed system. As a first step URL will be matched with the white-list and black-list databases. The system uses this approach to identify known phishing sites, and if it is a white-listed URL, the system allows the user to visit the website. If the URL does not exist in those databases, it will be sent to the URL analyzer. Then the URL analyzer will be predicted as a legitimate or phishing URL. Based on the prediction, the system will deny the website or moves to the webpage similarity comparison stage.

### IV. BROWSER EXTENTION

The system has a browser extension for the Chrome web browser that must be downloaded by the user. This plays a major role in system performance, which is explained below

### III. PROPOSED SOLUTION

In this section, the proposed phishing detection approach is explained. Phishing attacks have evolved a lot in past years such that even experienced users sometimes cannot be able to distinguish between phishing and legitimate pages. The proposed solution

#### a) Customized Whitelist and Blacklist

Users can categorize websites into a white list or black-list through the extension, and it will be saved in the extension. When the user is bookmarking a website, it will automatically be added to the user-customized white-list within the extension once the phishing detection is completed. Consequently, the extension itself can allow or deny accessing a website without check with the server-side.

#### b) Extracting the URL

Extracting URL from the website the user is trying to visit is done by the extension and then it is forwarded to the NoFish server for further analysis.

#### c) Capturing Image of the Current Website

The extension takes a screenshot of the current web site and redirects it to the NoFish server. The current web page image is required for log detection and web page similarity comparison; hence the screenshot is forwarded to the analysis.

### V. URL ANALYSIS

Many systems have been implemented to detect URL phishing attacks, and some of them have been focused mainly on email-based URL attacks only. However, phishing URLs can reach the victim in various ways. Nowadays, social media has become a major vector for phishing links. Very few of the existing solutions are still based on the old method, which is based on black-listing, and there are only a few existing systems that can-do real-time URL analysis to detect phishing attacks [14] [15]. However, they depend on language and algorithms that have been used to implement the system. The main purpose of implementing a URL analysis system such as NoFish is to detect any kind of phishing URL and secure the end-users as well as the organizations from phishing attacks better than prevailing solutions.

#### a) NoFish URL Analyzer

NoFish users can manage their own customized URL database in the extension. Therefore NoFish URL analyzer will not check URLs, which are in customized white-list and black-list available in the user browser extension, and it gives direct access to those sites. When a user browses a URL, which is not in customized data storage, the system request from the server to check it with a white-listed and a black-listed database. NoFish is not storing these databases, and it directly connects with the "Alexa" database and "Phish-Tank" database, and it uses their APIs to check the status of the URL. Alexa (Legitimate URLs) and Phish Tank (Phishing URLs) already maintain large databases orderly and authors believe it gives a better result and reduces the time to check compared to maintaining our own databases. However, according to user feedback, NoFish is maintaining its own white-listed and black-

listed database to personalize the service. The database is automatically updated according to user feedback. If that URL is not belonging to one of them, that means it is a newly identified URL from the analyzer. That URL goes through the trained machine learning model and give predictions whether it is phishing or legitimate. The system shows a warning to the user if the URL is phishing. Users can acknowledge and not continue or ignore the warning. If the model gives it as a legitimate URL, it is then immediately moved to the image classification and computer vision process.

#### b) Algorithms and Model

URL analysis is a common subject in the information security domain. There are so many existing projects on phishing detection on URL analysis and have used deep neural networks. However, NoFish has simply created its analyzer using Machine Learning (ML) approach after extensive research on several existing URL analyzers. It consists of Machine Learning algorithms and Natural Language Processing (NLP) [4] [14]. For measuring the performance of the system, a new dataset of phishing and legitimate URLs was constructed, and the experimental results were tested on them. NoFish have used Random Forest Classifier, Decision Tree Classifier, Logistic Regression Classifier, Support Vector Machine (SVM), and Naive Bayes algorithm with NLP feature and have done modifications and fine-tuning to create a higher accuracy model [16]. NoFish uses 13 features of URLs for identifying phishing patterns of a URL such as protocol, domain, path, having IP, long URL, short URL, redirection, prefix\_suffix-separation, sub domain, google index, DNS records, and https token. Test results are discussed in the *test results* section.

### VI. COMPUTER VISION FOR PHISHING DETECTION

This is one of the most important stages in the system, and the goal is to categorize websites to make it easier to compare with the legitimate website layouts [17]. Figure 2 depicts how the system uses computer vision to identify the current website.

#### a) Logo Detection

For this prototype, the logo detector can identify 20 image classes, including the most popular banks in Sri Lanka, and mostly used international websites. The logo detection model was trained using the Tensor Flow software library on Google Colab. NoFish team trained several Tensor Flow object detection models [16] with our own dataset, and in every case, it returned the same accuracy levels. Those models are mentioned in the *test results* section, along with the accuracy rates obtained.

Since the website login pages are not very complex images, the model can classify the logos with high accuracy. Therefore, we selected



faster\_rcnn\_inception\_v2\_coco as our logo detection model and train with our own dataset to identify 20 different logos with high accuracy.

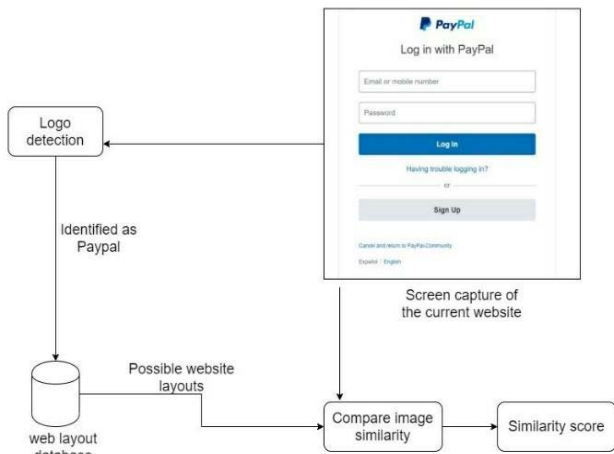


Figure 2: Flow Chart for Computer Vision

d) Compare Web Page Similarity

NoFish has developed this algorithm using the OpenCV python library to identify the similarity between the current website and the legitimate website. First, the algorithm identifies key points in both images and compares them to identify matching key points. Then defines a rating of similarity from 0 to 10, where 0 means they are completely different and 10 means they are perfectly matched. Based on the score, the system defines security levels. If the score is greater than 5 it defines as a high possibility, and if the score is greater than 3 and lower than 5 it will define as low possibility. Then the system returns a warning to the user accordingly, as depicted in Figure 3.

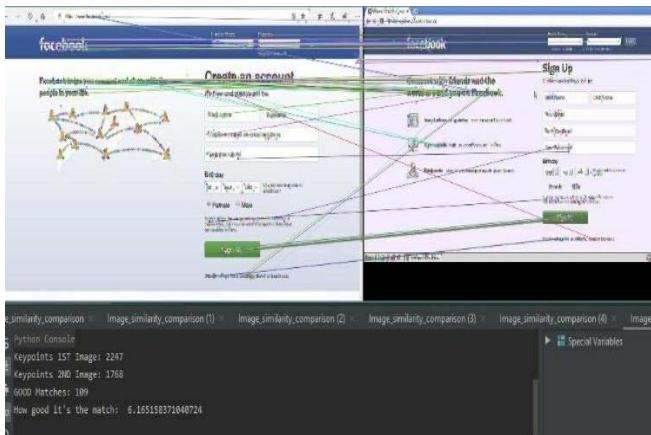


Figure 3: Image Comparison

## VII. EMAIL PHISHING DETECTION

Email phishing is a type of online scam where criminals ask users to provide sensitive information. This is mostly done by including a link that will appear to take you to the website that appears to be from a legitimate

company; however, the website is bogus. About 70% of phishing scandals involve national-state or state-affiliated actors, according to the Verizon 2018 Data Breach Investigations Report [18]. Phishing continues to be effective, more sophisticated, targeted, and difficult to identify. 4% of targeted people will click on the attachment, 94% of the time when the attachment is malicious. Only 17% of attacks are reported, and it usually takes 30 minutes to report. The cost of phishing for American businesses continues to grow, to more than half a billion dollars last year [1].

a) Proposed Model for Email Phishing Detection

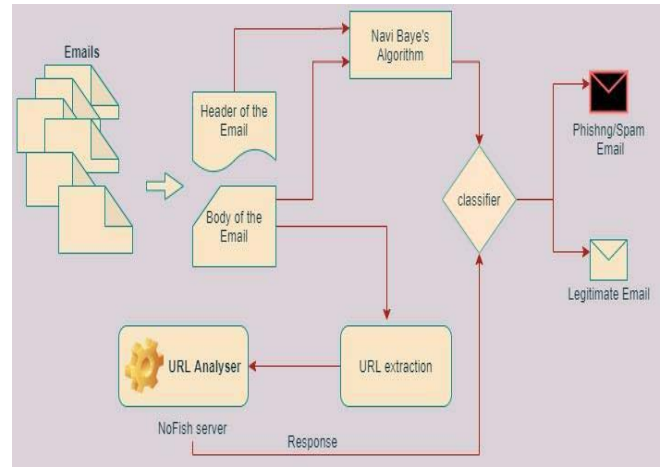


Figure 4: High-level Diagram for Client Email Plugin

NoFish email plugin for Microsoft Outlook email client has been proposed to prevent users from being victimized through email phishing attacks. As the below figure, the user needs to download the NoFish extension for the chrome browser. Then the user needs to install the email client plugin for Microsoft Outlook email client. Email plugin detects several ways of phishing emails. The email plugin detects spam emails for preventing the spams which are used by the phishers for attacks, and the plugin detects all the URLs in the email body to redirect to the existing URL analysis component to detect any phishing URLs. Detected spam emails are sent to the junk email folder, and phishing emails are blocked for users to view. A warning message will be notified for users about the phishing threat. The Yeoman generator, which is built with node.js, is used to create outlook add-in.

b) Detect spam emails

NoFish system detects for spam emails because phishing emails are also received as spams. It uses an algorithm called Naïve Bayes Classifier to detect if the email is spam or not [16]. Naïve Bayes is part of a large Natural Language Processing toolset and can be trained better when fed with many and complete spam emails [16][19]. They usually use a word bag to identify spam emails, a common approach to text



sorting. Naive Bayes classification works by associating tokens (usually words, or perhaps other things), spam and non-spam emails, and using Bayes' theorem to calculate the probability that an email is not spam [20]. This spam filter accesses the email account using the IMAP protocol. We experienced that most of the time, spam mostly comes from Chinese email hosts. Therefore, as a special feature, we use a function to scan all the characters in the subject text. It triggers on any character that falls into the Han Ideographs Unicode Range. It simply scans the complete range for Chinese characters in Unicode and detect if it is spam or not.

Bayes classifier sets up two categories to choose from. It contains possible spam sentences, phrases, and word-lists, which are weighted against a white list. This returns its verdict as either "spam" or "mail". It is implemented to open the folder named spam on the email account and delete all emails older than ten days.

Our team has tested both the Naïve Bayes Algorithm (20) and Support Vector Machine (SVM) algorithms to detect spam emails. According to the test results, the Naïve Bayes Algorithm was used to detect spam emails. Test results are discussed in the section *test results*.

## 2) Detect phishing URLs in emails

JavaScript libraries are used to detect URLs in the email body. URLs may hide in emails in several ways as attachments, texts, images etc. These URLs are detected and redirect to the existing system called URL Analysis to determine the URL is phishing or not. If the URL is phishing, the user is notified by a popup message and blocked the phishing email for viewing. Since the NoFish has an existing system to analyze phishing URLs in advance, the accuracy of detect phishing URLs is high. It protects users from zero-day phishing attacks [2].

## VIII. INTERACTIVE DASHBOARD

NoFish system provides a user interactive dashboard to enhance the user experience. Users may use the interactive dashboard through the official site. It provides features for the user to explore more services that are provided by NoFish systems, such as feedback mechanism. Users can vote for black-listed URLs to verify it as a phishing or malicious website. This may be used after installing NoFish extension to the web browser.

## IX. DETECTING DNS BASED ATTACKS

When the user is connecting to a WiFi network first, the system checks whether it was saved in the user's computer. If it is a saved WiFi system, assume that it is a trusted connection. When the user is connecting to a new WiFi network, then the system checks whether the WiFi connection requires a WPA or

WPA2 password. If not it is probably not secure. Further, to identify accurately, the system will ask the user whether it is public WiFi or trusted WiFi. If the WiFi is identified as untrusted, then the system will check for DNS related phishing attacks [12]. To identifying a fake DNS author [6] [5], proposed a solution that gives the IP address of the domain name of the current website using the IP Lookup API. Then using that IP address, the system can do a reverse IP lookup from the server-side and get the domain name, and by that, the system will define the DNS server is malicious or not [12][5].

## X. TEST RESULTS

In order to choose a model for logo detection our team trained several pertained models chosen from Tensor Flow object detection API with our own data set. Those models are mentioned below, along with the accuracy rates obtained.

- Faster\_rcnn\_inception\_v2\_coco model has a running time of 58ms per 600x600 image with mAP [<sup>^</sup>1] measure of 28 – over 95% accuracy.
- Ssd\_mobilenet\_v2\_coco model has a running time of 31ms per 600x600 image with mAP [<sup>^</sup>1] measure of 22 – over 95% accuracy.
- Faster\_rcnn\_inception\_resnet\_v2\_atrous\_coco model has a running time of 620ms per 600x600 image with mAP [<sup>^</sup>1] measure of 37 – over 95% accuracy.

When evaluating the URL analyzer, all the algorithms were tested separately with large phishing and legitimate data sets and Random Forest Classifier [21][22] returned 96.257%, Decision Tree Classifier returned 84.119%, Logistic Regression Classifier returned 91.037%, Support Vector Machine returned 91.002%, and Navy Bayes returned 94.128% accuracies respectively. Consequently, in order to obtain a better accuracy level, NoFish has ensemble all four algorithms together and created a finalized model combining NLP based features in it. NoFish uses 16 features of URLs for identifying phishing patterns of a URL. It gives nearly the best performance with a 94% model accuracy rate for the detection of phishing URLs.

According to past researches, SVM, and Naïve Bayes has more accuracy than other algorithms when detecting spam emails [16][9]. Within our calculation, SVM got 91.67%, and Naïve Bayes got 91.47% of accuracies, which shows the same accuracies. However, our team has identified SVM might not fast as other classification algorithms. Naïve Bayes classifier simply applies Bayes' theorem on the context of each email, with a strong assumption that the words included in the email are independent of each other. Therefore, NoFish has used the Naïve Bayes algorithm for spam detection with more success.

## XI. CONCLUSION AND RECOMMENDATIONS

In order to prevent phishing, business and consumers need to educate themselves about phishing and anti-phishing techniques. They should use current protection methods and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft and protect their privacy. The most effective solution for phishing is to train users not to blindly follow links to websites that need to include sensitive information such as passwords. The ultimate technological solution to phishing is the significant infrastructure changes on the Internet that exceed the ability of any organization to deploy. However, there are steps that can now be taken to reduce the consumer's risk of phishing attacks. Some of those steps are:

### For Corporations

- Provide a way for the consumer to validate that the email is legitimate.
- Stronger authentication on websites and emails.
- Implement a good quality anti-virus, anti-spam, and content filtering solutions at the internet gateway.

### For Consumers

Be suspicious.

- Automatically detect and block malicious emails, websites, URLs, and DNS servers.
- Automatically block sensitive information from leaking to malicious parties.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Lakhita, S. Yadav, B. Bohra, and Pooja, "A review on recent phishing attacks in Internet," in *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGIoT 2015*, 2016, pp. 1312–1315, doi: 10.1109/ICGC IoT.2015.7380669.
2. Carella, M. Kotsoev, and T. M. Truta, "Impact of security awareness training on phishing click-through rates," in *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, 2017, vol. 2018-January, pp. 4458–4466, doi: 10.1109/BigData.2017.8258485.
3. Tewari, A. K. Jain, and B. B. Gupta, "Recent survey of various defense mechanisms against phishing attacks," *J. Inf. Priv. Secur.*, vol. 12, no. 1, pp. 3–13, Jan. 2016, doi: 10.1080/15536548.2016.1139423.
4. E. Buber, B. Diri, and O. K. Sahingoz, "NLP Based Phishing Attack Detection from URLs," in *Advances in Intelligent Systems and Computing*, 2018, vol. 736, pp. 608–618, doi: 10.1007/978-3-319-76348-4\_59.
5. H. Kim and J. H. Huh, "Detecting DNS-poisoning-based phishing attacks from their network performance characteristics," in *Electronics Letters*, 2011, vol. 47, no. 11, pp. 656–658, doi: 10.1049/el.2011.0399.
6. "DNS Vulnerabilities," in *DNS Security Management*, John Wiley & Sons, Inc., 2017, pp. 57–83.
7. P. E. Rosiello, E. Kirda, C. Kruegel, and F. Ferrandi, "A layout-similarity-based approach for detecting phishing pages," in *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks, Secure Comm*, 2007, pp. 454–463, doi: 10.1109/SECCOM.2007.4550367.
8. H. Hsu, P. Wang, and S. Pu, "Identify fixed-path phishing attack by STC," in *ACM International Conference Proceeding Series*, 2011, pp. 172–175, doi: 10.1145/2030376.2030396.
9. H. Berger and D. Merkl, "A comparison of support vector machines and self-organizing maps for email categorization," *Aus DM 2005 Proc. - 4th Australas. Data Min. Conf. - Collocated with 18th Aust. Jt. Conf. Artif. Intell. AI 2005 2nd Aust. Conf. Artificial Life, ACAL 2005*, pp. 189–203, 2005.
10. Y. Huang, S. P. Ma, W. L. Yeh, C. Y. Lin, and C. T. Liu, "Mitigate web phishing using site signatures," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2010, pp. 803–808, doi: 10.1109/TENCON.2010.5686582.
11. S. Afroz and R. Greenstadt, "Phish Zoo: Detecting phishing websites by looking at them," in *Proceedings - 5th IEEE International Conference on Semantic Computing, ICSC 2011*, 2011, pp. 368–375, doi: 10.1109/ICSC.2011.52.
12. K. Gajera, M. Jangid, P. Mehta, and J. Mittal, "A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection," in *Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019*, 2019, pp. 196–200, doi: 10.1109/ICECA.2019.8822053.
13. L. Zhu, Z. Hu, J. Heidemann, D. Wessels, A. Mankin, and N. Somaiya, "Connection-oriented DNS to improve privacy and security," in *Proceedings - IEEE Symposium on Security and Privacy*, 2015, vol. 2015-July, pp. 171–186, doi: 10.1109/SP.2015.18.
14. O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Syst. Appl.*, vol. 117, pp. 345–357, Mar. 2019, doi: 10.1016/j.eswa.2018.09.029.
15. [15] R. Kiruthiga and D. Akila, "Phishing websites detection using machine learning," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 111–114, 2019, doi: 10.35940/ijrte.B1018.0982S1119.
16. T. Yang, K. Qian, D. C. T. Lo, K. Al Nasr, and Y. Qian, "Spam filtering using Association Rules and Naïve Bayes Classifier," in *Proceedings of 2015 IEEE International Conference on Progress in Informatics and Computing, PIC 2015*, 2016, pp. 638–642, doi: 10.1109/PIC.2015.7489926.

17. M. Hara, A. Yamada, and Y. Miyake, "Visual similarity-based phishing detection without victim site information," in *2009 IEEE Symposium on Computational Intelligence in Cyber Security, CICS 2009 - Proceedings*, 2009, doi: 10.1109/CICYBS.2009.4925087.
18. "1.4 Million New Phishing Sites Launched Each Month." [Online]. Available: <https://www.darkreading.com/threat-intelligence/14-million-new-phishing-sites-launched-each-month/d/d-id/1329955>. [Accessed: 23-Feb-2020].
19. Y. Fang, C. Zhang, C. Huang, L. Liu, and Y. Yang, "Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism," *IEEE Access*, vol. 7, pp. 56329–56340, 2019, doi: 10.1109/ACCESS.2019.2913705.
20. R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 324–335, Jan. 2013, doi: 10.1016/j.jnca.2012.05.009.
21. Usenix-security-submission, "An Image-based Feature Extraction Approach for Phishing Website Detection."
22. A. Subasi, E. Molah, F. Almkallawi, and T. J. Chaudhery, "Intelligent phishing website detection using random forest classifier," in *2017 International Conference on Electrical and Computing Technologies and Applications, ICECTA 2017*, 2017, vol. 2018-January, pp. 1–5, doi: 10.1109/ICECTA.2017.8252051.





This page is intentionally left blank



# QoS Evaluation of SIP Signalled VoIP Network Routed using MANET Routing Protocols

By N Shyam Sunder Sagar & P Chandrasekar Reddy

*GITAM University*

**Abstract-** A Mobile ad hoc network (MANET) is a type of network which consists of group of mobile nodes which are wireless and do not have fixed architecture. The nodes act as a router and depict the nature of dynamism. The three different classification of protocols in MANETS supports different applications. But to support real time applications like voice signalling and video signalling, we require the most efficient protocol that gives the QoS mechanism. Voice and video signalling demand to know the performance of different metrics in the network such as end-to-end delay, overall throughput of network and jitter of the network. This paper works on identifying and analyzing the performance of various protocols like AODV, DSR, OLSR and TORA which would help in fulfilling the mentioned need. Voice over Internet Protocol (VoIP), also known as IP telephony is a class of technologies used to deliver voice and multimedia sessions over internet protocol networks.

**Keywords:** MANET, Router, QoS, AODV, DSR, OLSR, TORA, VoIP, SIP.

**GJCST-E Classification:** C.2.2



*Strictly as per the compliance and regulations of:*





# QoS Evaluation of SIP Signalled VoIP Network Routed using MANET Routing Protocols

N Shyam Sunder Sagar<sup>α</sup> & P Chandrasekar Reddy<sup>σ</sup>

**Abstract-** A Mobile ad hoc network (MANET) is a type of network which consists of group of mobile nodes which are wireless and do not have fixed architecture. The nodes act as a router and depict the nature of dynamism. The three different classification of protocols in MANETS supports different applications. But to support real time applications like voice signalling and video signalling, we require the most efficient protocol that gives the QoS mechanism. Voice and video signalling demand to know the performance of different metrics in the network such as end-to-end delay, overall throughput of network and jitter of the network. This paper works on identifying and analyzing the performance of various protocols like AODV, DSR, OLSR and TORA which would help in fulfilling the mentioned need. Voice over Internet Protocol (VoIP), also known as IP telephony is a class of technologies used to deliver voice and multimedia sessions over internet protocol networks. The terms internet telephony, broadband telephony provides provisions over public internet networks rather than public switched telephone networks. Since the smart phones have evolve, VoIP has more popularity and its performance optimization has become a research interest. The VoIP network consisting of wireless nodes which are signalled through SIP are simulated with the help of OPNET Modeller 17.5. For the mentioned protocols which are useful in VoIP applications, their performance evaluations have been experimented and various conclusions have been put forth.

**Index Terms:** MANET, Router, QoS, AODV, DSR, OLSR, TORA, VoIP, SIP.

## I. INTRODUCTION

The MANET is a group of wireless nodes which are mobile in nature. They do not contain a central access point or any established infrastructure. Every node act as a router in order to establish communication between other entites in the network. These networks reflect dynamism which results irregular topology causing a complicated traffic among the nodes. The different protocols available are classified as reactive, proactive, hierarchical, flat, adaptive and geographical. Each of the above-mentioned category have their own set of protocols. Based on algorithmic designs the proactive and reactive protocols are most known. Each protocol has a unique nature and are designed differently. Routing efficiency has become a major issue in MANETS as they have mobile nodes. So, any protocol selected should be efficient in facing the

challenges posed by the network. Since each protocol is designed differently, they provide one or more than one solution to the challenges faced by the network Voice over Internet Protocol has been seen to gain immense popularity and is most common to most of the applications. The use of VoIP application is to such an extent that it has replaced most of the conventional telephone systems in the developed nations as VoIP has been found to be not so expensive and is compatible for systems to switch to new technologies. As understood, VoIP makes use of public internet for its communication so the input voice data is transformed to IP packets which are transmitted from source node to destination node through a secure channel using the protocol selected for its routing over the internet.

Various factors determine the VoIP QoS performance over MANET routing protocols which include mobility of nodes, voice codec, voice quality and distance between communicating pair, hop count, node capability, wireless LAN technology and duration of calls. The VoIP with GSM quality voice codecs has been considered, which has good quality of voice and performance over large varieties of systems and applications.

The main aim of paper is examining the QoS in SIP signaled VoIP application that uses MANET reactive routing protocols for its routing. The WLAN technology considered here is IEEE 802.11n which serves as physical layer technology. The nodes have been addressed through IPv4. The OPNET Modeller 17.5 is used for simulations. Both TCP and UDP based signalling of SIP has their impact on QoS in VoIP applications.

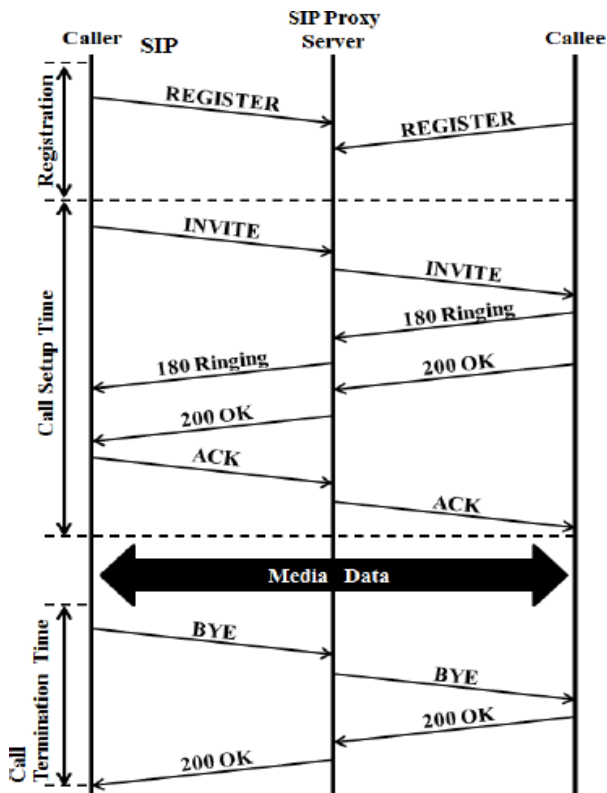
### a) SIP Signalling

Session Initiation Protocol is one of the common protocols used in VoIP technology. It belongs to application layer protocol that works in conjunction with other application layer protocols for the purpose of signalling and controlling multimedia applications like voice and video calls. The messages are sent between communicating pair i.e., the nodes to establish and terminate the calls among them. It is similar to HTTP and SMTP which involve message requests and message responses. So it is known as a text based protocol. It was defined by SIP working group and was published as IETF (RFC 2543). A SIP session may include more than one participant or application as it has internal

Author <sup>α</sup>: Assistant Professor, ECE Dept., GITAM University (Deemed), Hyderabad, India. e-mail: shyam428@gmail.com

Author <sup>σ</sup>: Professor, ECE Dept., JNTUH, Kukatpally, Hyderabad, India.

functionality to allow extensions and modifications. The various elements of SIP session are replicated by the changes in the code.



This protocol is dependent on internet protocols but independent of transport layer. A SIP based session or application consists of three stages. i. The Registration ii. The Initiation and iii. The Termination. The working of these stages depends on SIP proxy server for connectivity between nodes. The application performance is mostly affected due to delays which occur in the process of these stages. The acceptable average delay in a SIP system is in the range of [0.145, 0.345] seconds.

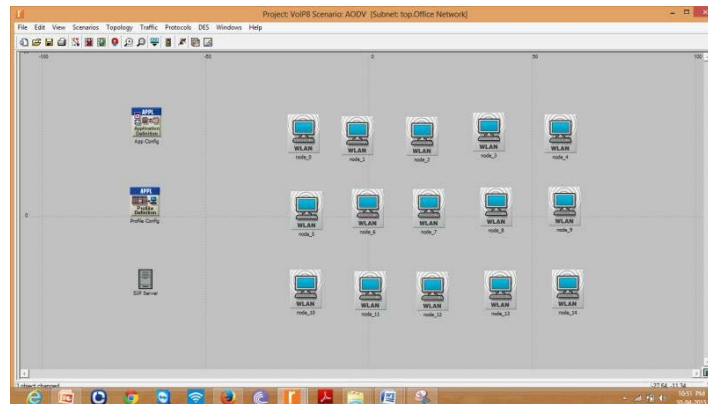
b) VoIP Applications

VoIP application is similar to using a microphone to record an audio message and storing it in a memory. In VoIP the message is not stored in a memory, rather it is disintegrated and transformed into IP packets which are transmitted over IP network. VoIP calls support any kind of device like a computer, a smart phone or a traditional telephone. The process of fragmentation into IP packets and then their transmission leads the packets to arrive in an arbitrary order. This reordering of packets is the issue as it may cause some of the packets to drop leading to silence in the calls for short time. The quality of VoIP calls depends on jitter, end-to-end delay, MOS value, throughput and coding schemes. A lot of research is being carried out in order to improve the reliability and quality of VoIP application. This paper discusses the different parameters that deteriorate the call quality.

c) MANET Routing Protocols

MANET is one of the growing and eminent technology in the field of telecommunication. It is self configured, infrastructure less, wirelessly connected without any central access point. In basic sense routing protocols are divided into Flat, Hierarchical, Geographic position assisted types. The flat routing protocols are further divided as proactive and reactive protocols. The Reactive routing protocols are the On-demand routing protocols which calculate the the routes when needed. These are AODV and TORA known as source-initiated route discovery protocols. On the other hand, proactive routing protocols calculate the shortest paths between nodes depending on updates on the routing tables. It includes OLSR and DSDV. The hybrid routing protocols contain the features and functionality of both proactive and reactive protocols.

II. VOIP NETWORK TOPOLOGY



Our main concentration is towards VoIP QoS, so mobility in nodes is ignored and are restricted to static model. The entire network is configured to function

as VoIP network with GSM application and voice codec as G711. Different scenarios have been created for different MANET routing protocol but the topology,

application configuration and other parameters have been kept constant so that we obtain an ideal comparison among the protocols used.

### III. SIMULATION PARAMETERS IN OPNET

|                               |         |                    |               |
|-------------------------------|---------|--------------------|---------------|
| Simulation Duration           |         | 10 Minutes         |               |
| Mobility Model                |         | Static             |               |
| MANET Routing Protocols       |         | DSR,AODV,OLSR,TORA |               |
| No. of Nodes                  | 16      | Area Dimension     | 100 m x 100 m |
| WLAN Physical Characteristics |         | IEEE 802.11n       |               |
| Data Rate                     |         | 13 Mbps            |               |
| Frequency Range               | 2.4 GHz | Transmission Power | 0.001 W       |
| Packet Size                   | 512 B   | Buffer Size        | 32 Kb         |

OLSR Parameters

|                                       |    |                               |      |
|---------------------------------------|----|-------------------------------|------|
| Hello Interval (Seconds)              | 3  | Neighbour Hold Time (Seconds) | 6    |
| TC Interval (Seconds)                 | 5  | Topology Hold Time (Seconds)  | 15   |
| Duplicate Message Hold Time (Seconds) | 10 | Addressing Model              | IPv4 |

AODV Parameters

|                          |                 |                                |      |
|--------------------------|-----------------|--------------------------------|------|
| Hello Interval (Seconds) | Uniform (1,1.1) | Active Route Timeout (Seconds) | 3    |
| Allowed Hello Loss       | 2               | Node Traversal Time (Seconds)  | 0.04 |

|                        |    |                |   |
|------------------------|----|----------------|---|
| Route Error Rate Limit | 10 | Timeout Buffer | 2 |
|------------------------|----|----------------|---|

DSR Parameters

### IV. SIMULATIONS

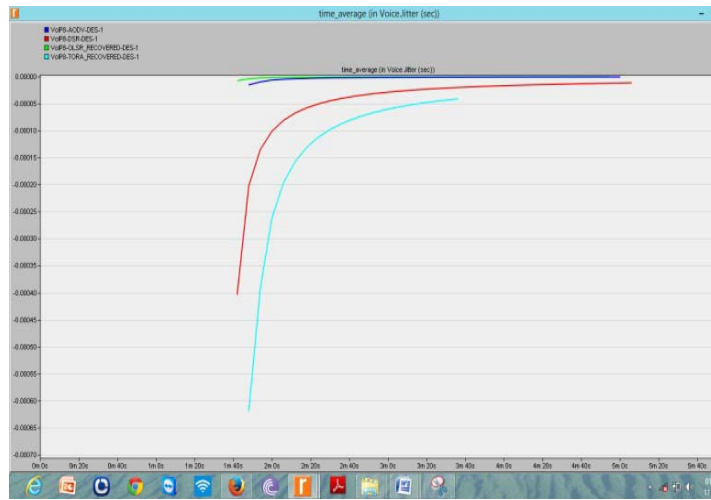
The software used for simulations of VoIP network is OPNET Modeller 17.5. the simulation consists of an office setup with dimension of 100x100 metres. The technologies selected from the dropdown menu are MANET, SIP and Voice Signalling. The wireless LAN workstations are selected from the object palette as user nodes and are placed in the workspace provided. A SIP proxy server is selected as network node. The application configuration attributes are edited and are set to voice application. The attributes are changed to GSM voice application with voice codec G711. The user profiles are created using profile configuration.

### V. RESULTS AND EVALUATIONS

The simulation results are provided in two groups as – the Voice statistics and the wireless LAN characteristics. The parameters jitter, MOS value and packet end-to-end delay come under the voice statistics and the throughput and delay come under WLAN characteristics. All statistics are found under global statistics of the modeler. The traffic sent and the traffic received are also analysed through the simulation. In the graphs obtained, the horizontal axis depicts the simulation time in seconds and vertical axis depict the values of evaluated statistics which include jitter, throughput, MOS value, etc. The total simulation time is set to 600 seconds, in which the initial results of first 150 simulation seconds are difficult to analyse. Therefore, only rest of the 450 simulation seconds are taken into consideration for estimation of performance of application under different conditions.



a) Voice Signalling Statistics:  
Jitter (Seconds)



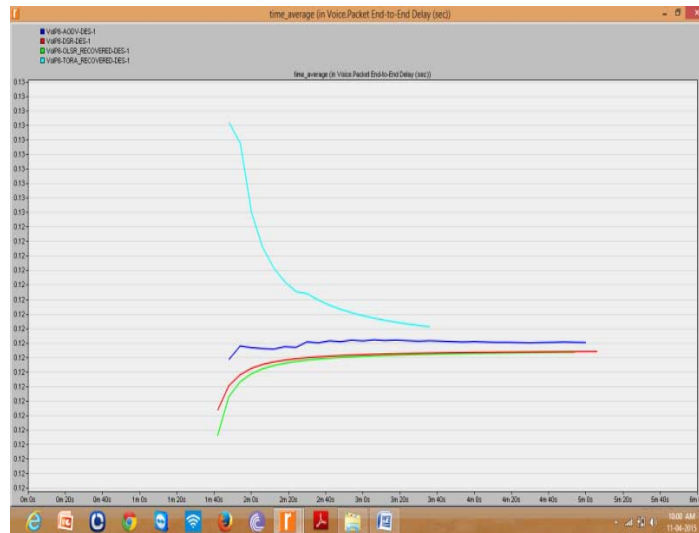
The following graphs show the time averaged jitter values of the VoIP signal with the different MANET protocols.

If two packets leave the source node at time interval t1 and t2, the same packets replay at the receiver at time interval t3 and t4 respectively, then the jitter is (t4-t3)-(t2-t1). Negative jitter indicates that the

time difference between the packets at destination loads is less than that at the source node.

Packet end-end delay

The following graph represents the time averaged packet end to end delay of the VoIP network over the MANET routing protocols.



MOS Value

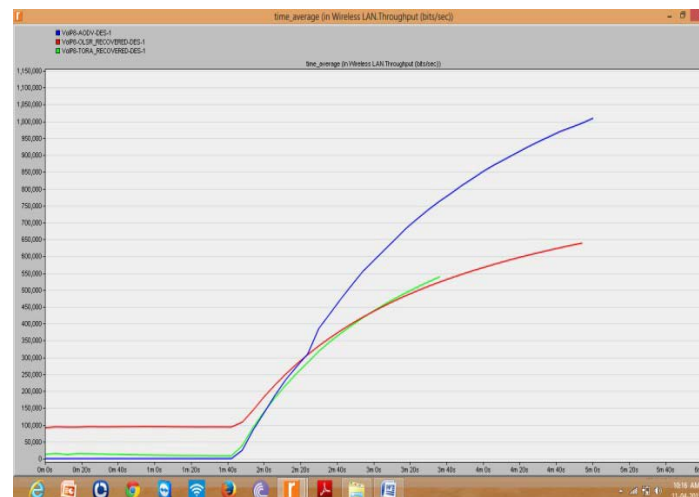
The following graph represents the time averaged MOS value of the VoIP network over the MANET routing protocols.





b) WLAN Statistics  
Throughput

The following graph represents the throughput values of the VoIP network when routed through the MANET Routing Protocols.



VI. CONCLUSIONS

The above study gives a clear idea of various parameters of VoIP network routed through three reactive protocols: DSR, AODV and TORA and a proactive protocol: OLSR. This segment of paper talks about the behavior of each protocol at different simulation time intervals.

To start with jitter values, we observe that DSR and TORA have negative jitter values whereas OLSR and AODV have almost zero jitter value. This tells us that frequency of IP packets at receiver end is small compared to source end. The receiver end is also noticed to face difficulty in synchronizing and reattaching the received packets. In terms of real time applications, jitter is found to be not a good parameter to be considered for knowing the quality of voice. Keeping in mind the above problem, OLSR and AODV dominate the other protocols.

In the initial time period of 120 seconds, the packet end-to-end delay was found to be low when DSR, AODV and OLSR were used. But after 120 simulation seconds, it increased and maintained constant value. On the contrary, in case of TORA same statistic was high in the initial and decreased as simulation came to an end. As delay cannot be entertained in voice applications, use of TORA has been avoided. Among the other three protocols we cannot conclude on the better among them as they have minimal difference.

Higher is the Mean Opinion Score that better is any application. From the graphs, it is very clear that the protocols DSR and OLSR have an unbeatable MOS value compared to that of AODV and TORA. The AODV initially maintained a good score but that didn't maintain longer. The TORA routed network performed the least among all the protocols considered. In this context, the usage of AODV and TORA are strictly not



recommended. Taking all the above three observations into consideration, among the four MANET routing protocols considered, from the reactive routing protocols, the DSR is observed to be the optimal one to use for the voice applications and on the other side, among the proactive routing protocols, the only considered Optimized Link State Routing protocol managed to perform equally as the DSR. Hence, the paper suggests the usage of both the DSR and the OLSR based on the requirements of the application end.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. K. Pandey and A. Swaroop, "A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid MANETs Routing Protocols," IJCSI International Journal of Computer Science Issues, Vol. 8, No.3, 2011.
2. Mazin Alshamrani, Haitam Cruickshank, Zhili Sun, Vahid Fami, and Bansil Elmasri, " Evaluation Of SIP Signalling and QoS for VoIP Over MANETS Reactive Routing Protocols," 2013.
3. Hetal Jasani, "Quality of Service Evaluations of On Demand Mobile Ad-HOC Routing Protocols," 2011.
4. S. Ganguly and S. Bhatnagar, "VoIP: Wireless, P2P and New Enterprise Voice over IP," Chichester, England: Wiley, 2008. Print.
5. Farukh Mahmudur Rahman and Mark A Gregory, "IP Address Associated 4-N Intelligent MANET Routing Algorithm utilising LTE Cellular Technology,".
6. C. Perkins (Ed.), Ad hoc Networking, Addison Wesley, 2001.
7. C. Liu, J. Kaiser, "A Survey of Mobile Ad Hoc network Routing Protocols", Technical Report (Nr. 2003-08) Uni versity of Ulm, Germany, 2003.
8. Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, (2003) "Mobile ad hoc networking: imperatives and challenges", Adhoc Networks, Elsevier, pp. 13-64.



# GLOBAL JOURNALS GUIDELINES HANDBOOK 2020

---

[WWW.GLOBALJOURNALS.ORG](http://WWW.GLOBALJOURNALS.ORG)

# MEMBERSHIPS

## FELLOWS/ASSOCIATES OF COMPUTER SCIENCE RESEARCH COUNCIL FCSRC/ACSRC MEMBERSHIPS

### INTRODUCTION



FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

### FCSRC

#### FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.



## BENEFIT

### TO THE INSTITUTION

#### GET LETTER OF APPRECIATION

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.



### EXCLUSIVE NETWORK

#### GET ACCESS TO A CLOSED NETWORK

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career

Credibility

Exclusive

Reputation



### CERTIFICATE

#### CERTIFICATE, LOR AND LASER-MOMENTO

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career

Credibility

Exclusive

Reputation



### DESIGNATION

#### GET HONORED TITLE OF MEMBERSHIP

Fellows can use the honored title of membership. The "FCSRC" is an honored title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career

Credibility

Exclusive

Reputation

### RECOGNITION ON THE PLATFORM

#### BETTER VISIBILITY AND CITATION

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career

Credibility

Reputation

## FUTURE WORK

### GET DISCOUNTS ON THE FUTURE PUBLICATIONS

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career

Financial



## GJ ACCOUNT

### UNLIMITED FORWARD OF EMAILS

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career

Credibility

Reputation



## PREMIUM TOOLS

### ACCESS TO ALL THE PREMIUM TOOLS

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

## CONFERENCES & EVENTS

### ORGANIZE SEMINAR/CONFERENCE

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career

Credibility

Financial

## EARLY INVITATIONS

### EARLY INVITATIONS TO ALL THE SYMPOSIUMS, SEMINARS, CONFERENCES

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive







## PUBLISHING ARTICLES & BOOKS

### EARN 60% OF SALES PROCEEDS

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive

Financial

## REVIEWERS

### GET A REMUNERATION OF 15% OF AUTHOR FEES

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

## ACCESS TO EDITORIAL BOARD

### BECOME A MEMBER OF THE EDITORIAL BOARD

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career

Credibility

Exclusive

Reputation

## AND MUCH MORE

### GET ACCESS TO SCIENTIFIC MUSEUMS AND OBSERVATORIES ACROSS THE GLOBE

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

## ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.



## BENEFIT

### TO THE INSTITUTION

#### GET LETTER OF APPRECIATION

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.



### EXCLUSIVE NETWORK

#### GET ACCESS TO A CLOSED NETWORK

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly. They should also be open to reaching out by other.

Career

Credibility

Exclusive

Reputation



### CERTIFICATE

#### CERTIFICATE, LOR AND LASER-MOMENTO

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career

Credibility

Exclusive

Reputation



### DESIGNATION

#### GET HONORED TITLE OF MEMBERSHIP

Associates can use the honored title of membership. The "ACSRC" is an honored title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career

Credibility

Exclusive

Reputation

### RECOGNITION ON THE PLATFORM

#### BETTER VISIBILITY AND CITATION

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career

Credibility

Reputation

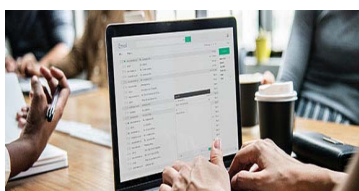
## FUTURE WORK

### GET DISCOUNTS ON THE FUTURE PUBLICATIONS

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career

Financial



## GJ ACCOUNT

### UNLIMITED FORWARD OF EMAILS

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career

Credibility

Reputation



## PREMIUM TOOLS

### ACCESS TO ALL THE PREMIUM TOOLS

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

## CONFERENCES & EVENTS

### ORGANIZE SEMINAR/CONFERENCE

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career

Credibility

Financial

## EARLY INVITATIONS

### EARLY INVITATIONS TO ALL THE SYMPOSIUMS, SEMINARS, CONFERENCES

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive





## PUBLISHING ARTICLES & BOOKS

### EARN 30-40% OF SALES PROCEEDS

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive

Financial

## REVIEWERS

### GET A REMUNERATION OF 15% OF AUTHOR FEES

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

## AND MUCH MORE

### GET ACCESS TO SCIENTIFIC MUSEUMS AND OBSERVATORIES ACROSS THE GLOBE

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.





| ASSOCIATE                                                                                                                                                                                                               | FELLOW                                                                                                                                                                                                                                                                | RESEARCH GROUP                                                                                                                                                                                                                                                        | BASIC                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| <p>\$4800<br/>lifetime designation</p> <hr/> <p>Certificate, LoR and Momento<br/>2 discounted publishing/year<br/>Gradation of Research<br/>10 research contacts/day<br/>1 GB Cloud Storage<br/>GJ Community Access</p> | <p>\$6800<br/>lifetime designation</p> <hr/> <p>Certificate, LoR and Momento<br/>Unlimited discounted publishing/year<br/>Gradation of Research<br/>Unlimited research contacts/day<br/>5 GB Cloud Storage<br/>Online Presense Assistance<br/>GJ Community Access</p> | <p>\$12500.00<br/>organizational</p> <hr/> <p>Certificates, LoRs and Momentos<br/>Unlimited free publishing/year<br/>Gradation of Research<br/>Unlimited research contacts/day<br/>Unlimited Cloud Storage<br/>Online Presense Assistance<br/>GJ Community Access</p> | <p>APC<br/>per article</p> <hr/> <p>GJ Community Access</p> |



# PREFERRED AUTHOR GUIDELINES

**We accept the manuscript submissions in any standard (generic) format.**

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from <https://globaljournals.org/Template.zip>

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at [submit@globaljournals.org](mailto:submit@globaljournals.org) or get in touch with [chiefeditor@globaljournals.org](mailto:chiefeditor@globaljournals.org) if they wish to send the abstract before submission.

## BEFORE AND DURING SUBMISSION

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct*, along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s) names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

## Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

## POLICY ON PLAGIARISM

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures



- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

## AUTHORSHIP POLICIES

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

### Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

### Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

### Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

### Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

### Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

## PREPARING YOUR MANUSCRIPT

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.



### ***Manuscript Style Instruction (Optional)***

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

### ***Structure and Format of Manuscript***

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

- a) A title which should be relevant to the theme of the paper.
- b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
- c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
- d) An introduction, giving fundamental background objectives.
- e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
- f) Results which should be presented concisely by well-designed tables and figures.
- g) Suitable statistical data should also be given.
- h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

- i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
- j) There should be brief acknowledgments.
- k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.



## FORMAT STRUCTURE

***It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.***

All manuscripts submitted to Global Journals should include:

### **Title**

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

### **Author details**

The full postal address of any related author(s) must be specified.

### **Abstract**

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

### **Keywords**

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in a research paper?" Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

### **Numerical Methods**

Numerical methods used should be transparent and, where appropriate, supported by references.

### **Abbreviations**

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

### **Formulas and equations**

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

### **Tables, Figures, and Figure Legends**

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.





## Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

## PREPARATION OF ELETRONIC FIGURES FOR PUBLICATION

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

## TIPS FOR WRITING A GOOD QUALITY COMPUTER SCIENCE RESEARCH PAPER

Techniques for writing a good quality computer science research paper:

**1. Choosing the topic:** In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

**2. Think like evaluators:** If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

**3. Ask your guides:** If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

**4. Use of computer is recommended:** As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

**5. Use the internet for help:** An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.



**6. Bookmarks are useful:** When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

**7. Revise what you wrote:** When you write anything, always read it, summarize it, and then finalize it.

**8. Make every effort:** Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

**9. Produce good diagrams of your own:** Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

**10. Use proper verb tense:** Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

**11. Pick a good study spot:** Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

**12. Know what you know:** Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

**13. Use good grammar:** Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

**14. Arrangement of information:** Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

**15. Never start at the last minute:** Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

**16. Multitasking in research is not good:** Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

**17. Never copy others' work:** Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

**18. Go to seminars:** Attend seminars if the topic is relevant to your research area. Utilize all your resources.

**19. Refresh your mind after intervals:** Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.



**20. Think technically:** Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

**21. Adding unnecessary information:** Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

**22. Report concluded results:** Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

**23. Upon conclusion:** Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium through which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

## INFORMAL GUIDELINES OF RESEARCH PAPER WRITING

### **Key points to remember:**

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

### **Final points:**

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

*The introduction:* This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

### **The discussion section:**

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

### **General style:**

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

**To make a paper clear:** Adhere to recommended page limits.



### *Mistakes to avoid:*

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

### **Title page:**

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

**Abstract:** This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

*Reason for writing the article—theory, overall issue, purpose.*

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

### **Approach:**

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

### **Introduction:**

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.



*The following approach can create a valuable beginning:*

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

#### **Approach:**

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

#### **Procedures (methods and materials):**

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

#### **Materials:**

*Materials may be reported in part of a section or else they may be recognized along with your measures.*

#### **Methods:**

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

#### **Approach:**

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

#### **What to keep away from:**

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.





**Results:**

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

**Content:**

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

**What to stay away from:**

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

**Approach:**

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

**Figures and tables:**

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

**Discussion:**

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."



Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

**Approach:**

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

## THE ADMINISTRATION RULES

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

*Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.*

*Segment draft and final research paper:* You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

*Written material:* You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.



CRITERION FOR GRADING A RESEARCH PAPER (COMPILATION)  
BY GLOBAL JOURNALS INC. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

| Topics                        | Grades                                                                                                                                                                                 |                                                                                                     |                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
|                               | A-B                                                                                                                                                                                    | C-D                                                                                                 | E-F                                                                |
| <i>Abstract</i>               | Clear and concise with appropriate content, Correct format. 200 words or below                                                                                                         | Unclear summary and no specific data, Incorrect form<br><br>Above 200 words                         | No specific data with ambiguous information<br><br>Above 250 words |
| <i>Introduction</i>           | Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited | Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter | Out of place depth and content, hazy format                        |
| <i>Methods and Procedures</i> | Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads                                                              | Difficult to comprehend with embarrassed text, too much explanation but completed                   | Incorrect and unorganized structure with hazy meaning              |
| <i>Result</i>                 | Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake                                         | Complete and embarrassed text, difficult to comprehend                                              | Irregular format with wrong facts and figures                      |
| <i>Discussion</i>             | Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited                                               | Wordy, unclear conclusion, spurious                                                                 | Conclusion is not cited, unorganized, difficult to comprehend      |
| <i>References</i>             | Complete and correct format, well organized                                                                                                                                            | Beside the point, Incomplete                                                                        | Wrong format and structuring                                       |



# INDEX

---

---

## **A**

Appropriate · 5, 18, 19, 74, 86

---

## **C**

Credentials · 26, 37

---

## **E**

Emitting · 4, 9, 10  
Engines · 18  
Enlarged · 5

---

## **I**

Illustrates · 4, 10  
Implemented · 2, 4, 8, 20  
Inordinate · 4  
Intrusiveness · 4, 5, 6

---

## **P**

Protocol · 1, 51, 60, 67, 69, 70, 71

---

## **R**

Revolutionary · 6

---

## **S**

Sensing · 2, 6



save our planet



# Global Journal of Computer Science and Technology

---

Visit us on the Web at [www.GlobalJournals.org](http://www.GlobalJournals.org) | [www.ComputerResearch.org](http://www.ComputerResearch.org)  
or email us at [helpdesk@globaljournals.org](mailto:helpdesk@globaljournals.org)



ISSN 9754350