A Novel Hifi-Hacking Interrupter for Iot Devices

Bhadra Priya S S, Nishi S Das

***Abstract:** Internet of Things (IoT) is a very relevant technology used by internet networks to send and receive sensed data via a sensor. The same relates to common data communication except that sensors and microcontrollers are commonly used in IoT. It is supposed to explore, and there will be developing interest in the IoT framework which gives frequent IoT system capabilities. It connects us to the Internet and also helps us to reveal and manage the actual world by using sharing its info. IoT systems make use of real-world data, so device-collected data may also be a tool for cyber attack. The attack surface also expands as IoT expands and all the vulnerabilities present in the digital world flow through our modern world. DDoS attacks built on compromised IoT systems emerge as a serious problem. There are many technological solutions, but technology has changed a lot, so software solution can be in risk as well. The proposed system will serve as a prevention tool for DDoS attack and send the admin an alert when an attempt is made to hack the IoT device. In this proposed system, intend to provide a highly secured platform that will clean out all the unnecessary data without disrupting IoT's normal operation.*

***Keywords:** DDoS Attack, HiFi, Internet of Things, MQTT, NodeMCU, Security of IoT*

I. INTRODUCTION

The IoT is a rising apace, and with the aid of 2022 is expected to consist of 18 billion connected devices. But the speculation that shaped the history to the Internet's primitive creation no longer follow in the early stages of IoT development [1].IoT (Internet of Things) is a cutting -edge technology for transmitting sensor data obtained by internet networks. It is just like normal communication with data except that usually sensors and microcontrollers are used in IoT. from the devices are often immediately redirected into the The transmitting and receiving of data does not depend on the system, but depends on tools such as cell phones, messaging pads or even smart watches that are known to be microcontrollers and handheld communication devices. In IoT, most data cloud. This is typically accomplished when the microcontroller is attached to Wi-Fi and for this reason the microcontroller is connected to Wi-Fi [2].

The internet began in an atmosphere of mutual confidence wherever anyone could read, alter or inject knowledge. But IoT begins in a hostile environment wherever public and government demands are strong in terms of protection and privacy, and data security is a major concern among IoT adopters [3].IoT (Internet of Things) may be a kind of collaborative environment that is connected to smart and context-aware devices. It seemed successful because, contrasting with the Ubiquitous, the major part of the 4th Industrial Revolution supported the rapid development of the cloud, communication technologies, sensor, etc. Protecting information will become the biggest threat to IoT's existence. IoT creates and makes unimaginable amounts of physical objects, spaces, and people data available. With theadvancementof electronic technology and consumer market trends in previous decades, IoT devices play a significant role in our lives and are becoming increasingly sophisticated, networked, and functionally software-extendable. Since the security of the IoT device [4] is in urgent need, and particularly the software attack has become the biggest threat.However, the IoT is not without its disadvantages: there is only software that secures the systems that can still be hacked and hardware solutions only in the form of architectural techniques and these devices are also a common weapon in extremely destructive attacks on Distributed Denial-of-Service (DDoS). Commonly DDoS attacks are evaluated by considering three layer which are Perception, Network and Application Layer [5] DDoS attacks have been made over the last few weeks with 145,000 IOT-compatible cameras (web cameras, security cameras, etc.) collected by cyber hijackers [6]. They only detect the threat and there are nopreventive measures. It will break the IoT function while a large data flow occurs. It is not that much safe to install. Botnet attacks and DDoS attacks and the security of the IoT system in general were reviewed in[7].Botnets are used by cyber criminals to launch botnet attacks, including malicious activities such as password leaks, unauthorized access, data theft and DDoS attacks. Prokofiev et al [8] inorder developed a logistic regression model towards spotting botnet attacks. Accuracy, F-measure precision was calculated inorder to determine the model's effectiveness. Cusack et al. [9] performed a pilot study to find vulnerabilities and provide recommendations for the safety of camera surveillance systems. PointGuard strategy is implemented in [10] and HSD defender technique has been used for defending buffer overflow attacks [11].In this paper, proposed a hardware enhanced technique which possess fine physical isolation, high operation performance and low resource overhead, which is more efficient than existing systems. In these new methods, we introduced a device which will act like a hack preventing module and gives an alert to the admin when an attempt is made to hack the IoT device.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author

BhadraPriya S S*, UG Student, ECE Department Trinity college of Engineering, Naruvamoodu, Trivandrum, Kerala, India

Nishi.S.Das, Asst.Professor, ECE Department, Trinity college of Engineering, Naruvamoodu, Trivandrum, Kerala ,India.

Retrieval Number: D8323049420/2020©BEIESP
DOI: 10.35940/ijeat.D8323.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication
© Copyright: All rights reserved.

It will filter out all the unwanted data that enter into the device and will never

crash the IoT device or its data. It helps in identifying the hacking sources that enter into the IoT device. Comparison for the related work is shown in Table1.

II. SYSTEMMETHODOLOGY

This paper explains the importance of proposed IoT (Internet of Things) program in the field. The protection of the IoT device is in urgent need and especially the software attack has become the greatest threat. A common trend in security attacks on software is that program bugs are exploited to result in unpredictable actions by modifying the original integrity information to execute the malicious code, which causes both sensitive data leakage and malicious code execution changed. The sophisticated intruder may monitor the address or data bus by using advanced electronic equipment to manipulate or alter the instruction code, disrupt the communication between the processor and the main memory, and monitor the execution in the direction he wishes. The architecture is developed with a view to defending an IoT network against vulnerabilities.

Table-I: Comparison for the related work

Author	Method	Software	Purpose	
Osuwa et al. [2]		Artificial Intelligence Data mining, manage and control in the network		C language of congestion
Xu et al. [4]	Architectural security enhanced hardware design	To avoid buffer overflow attack		
OR1200-FPGA Platform				
Oh et al. [6]	Oauth2.0-basedoneM2M	Authentication and Authorization Thing Adaptor and Software		
Prokofiev [8]	Logistic Regression Model	-	To detect IoT Botnets	
Cowan et al [10]		PointGuard		GCCcompiler

Fig. 1 displays the block diagram for the framework beingproposed. The proposed IoT system consists of a temperature sensor and relay module which is suitable for home automation andboth are operated by a Node MCU. Thus, an app named HiFihas been successfully developed which allows us to track the real-time temperature of the region where the DHT11 temperature sensor is located and also to accesscontrol.

A. Temperature Sensor

DHT11 humidity sensor has been used. It is coded in Node MCU and in degree Celsius the room temperature is continuously monitored. It ensures the good reliability and excellent consistency over the long term. It attaches to a high performance 8-bit microcontroller. This sensor includes a resistive feature and sensation of measuring devices for wet NTC temperature. It has excellent consistency, rapid reaction, anti-interference, excellent quality, fast response, anti-interference ability and high cost performance advantages. Fig. 2.shows DHT11 temperature sensor and its specification is indicated in Table 2.

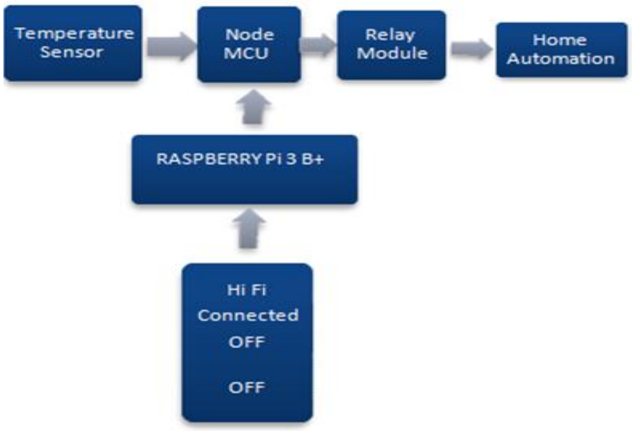


Fig. 1. Block Diagram of System

B. NodeMCU

Node MCU's development board is a flexible tool for microcontroller programming, and is part of the IoT. This includes Espressif Systems firmware running on the P8266 Wi-Fi SoC, andESP-12 related hardware. The framework uses Lua scripting language. This uses other open source projects including lua-cjso, and SPIFFS.Fig.3.shows an ESP8266 NodeMCU configuration with its pinconfiguration.

Fig.2. DHT11 Temperature sensor [12]

Relay Module

IoT Power Relay is a manageable power module provided with four outputs to help make the IoT a safe and reliable power control project. With the IoT Power Circuit, we can control the power to a system easily from an Arduino, Raspberry Pi or any other single- board machine or microcontroller. Fig. 4 shows model of four channel relay module.

C. Home Automation

It controls lighting and appliances. And also includes an alarm security system. Programmed on Node MCU. It is connected to 4 channel 5V relay module.

Retrieval Number: D8323049420/2020©BEIESP
DOI: 10.35940/ijeat.D8323.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

D.RASPBERRY PI 3B+

Raspberry Pi is a miniature board composed of a fixed processor chip with several peripheral USB ports, camera, SD cards, HDMI cable, etc. The Raspberry Pi (3 B) is a 3rd generation model that retains the same standard board configuration as the Raspberry Pi (2) and Raspberry Pi (B+), but features a 1.2GHz 64Bit SOC faster on board, and WiFi and Bluetooth. The Raspberry Pi 3 has a chip-based Broadcom BCM2835 device that includes an ARM11 700 MHz processor, VideoCore IV GPU. It does not have a built-in hard disk or solid-state drive, but uses an SD card for booting and permanent storage, while the Model B+ uses a Micro SD. The Foundation provides downloadable updates for the Debian and Arch Linux ARM. The Raspberry Pi (3) has a similar form factor to the previous Pi 2 and is fully compatible with Pi 1 and 2. A 2.5 Ampere power Supply is recommended for the Pi 3. The specification for the 3 B+ is given in Table 3.

Fig.3.Model of NodeMCU ESP8266 and Pin

Table- II: Specification of DHT11 Temperature Sensor

Sl.No	Parameter	Range
1	Supply Voltage	+5V
2	Temperature Range	0-5 degree celcius
3	Humidity	20-90% RH
4	Interface	Digital

Table-III:Raspberry Pi Specifications

Sl.No	Parameter	Specification
1	System on Chip	Raspberry Pi 3B +
2	Architecture	ARMv8
3	Core Type	Quad Core
4	GPU	Video Core IV
5	Memory	1 GB DDR2
6	CPU Clock	1.5 GHz

III. SOFTWARE REQUIREMENT

A. Python

Python was the programming language used to construct the attachment device. The explanation for this is Python is an acceptable scripting language for penetration testing since Pythonis a cross-platform object-oriented language that has a large library system. Py Charm Community Edition 2018.1.3 was used for programming.

B. Node Programming

Node MCU is implemented in C and is based on the SDK of Espressif NON-OS. Node MCU programming model in Luajust resembles Node.js programming model. It is asynchronous, and driven by events. But some functions have parameters for callback functions.

IV.IMPLEMENTATION AND DISCUSSION

The goal of this product is to provide a highly protected system that will serve as a link between the IoT devices and the cloud. Raspberry Pi is utilized as the mother of HiFi. An Android appwas created using Android Studio named HiFi to analyze the data. The work focuses specifically on DDoS attacks so that HiFi can detect it when the excess data flow occurs into the IoT devices and block the data flow into the IoT device. So when an approved data arrives it will be able to move through the Pi if an unauthorized data push comes then it will be immediately removed and the data will be saved in a separate file within the Raspberry Pi. For more information on the sender's identity, this data can be further analyzed, and the IP address of the sender can also be tracked, and further data entry from that source can be blocked.

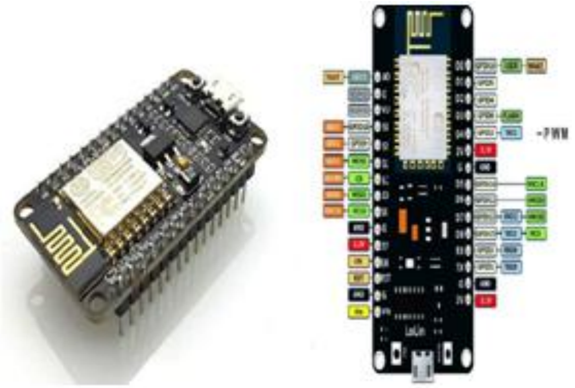


Fig.5. Photograph of System Implementation

Raspberry PI (3 b+) was initially set up and Raspbian OS was installed in it. For more programming, we use the Message queuing telemetry transmission (MQTT) protocol, as it helps to avoid DDoS attacks. The Raspberry is built as a hotspot here in HiFi, and it functions as a server-client relationship where the sever is the PI itself and the client seems to be the IoT devices and the HiFi App. Thus configured the PI by using MQTT protocol. And built the PI for server feature. Using the MQTT protocol, the server used for that is mosquito server. For the ease of use, a client-server protocol is used in HiFi.MQTT is an ISO standard for publishing subscribes messaging protocols. It functions on top of TCP/IP protocol. MQTT is seen as a messaging protocol that offers a fairly simple way to identify telemetry information for resource-constrained customers on the network. The protocol is used for machine-to-machine correspondence, and uses a correspondence pattern for publishing / subscribing. So Raspberry PI was designed to function as a server. Then created two folders of files within the PI so that one of them contains the correct data while the other one contains the false data that is the hacking files.

The hacked file includes invalid data arriving to our IoT units.

Distributed Denial- of-Service (DDoS) might attack a target server or network's normal traffic by flooding the target or its surrounding networks with an Internet traffic burst. Fig. 5 Shows Picture of Device Implementation.

V. RESULT

To test the HiFi system output, two IoT devices are connected, one is a home automation system and the other is a temperature sensor system. It is necessary to observe the initial part of the configurations, the following libraries, the ESP8266 WiFi command which allows the system to be configured with a MQTT server.

```
#include <ESP8266WiFi.h>
#include <PubSubClient.h>0
const char* ssid = "Redmi";
const char* password = "qwerty123";
const char* mqtt_server = "iot.eclipse.org";
```

The main focus of home automation is on a visual-based performance. The relay system is configured and various commnads for ON and OFF operations are allocated. The output is shown in Fig. 10 when one relay in On and Off. The Controller computer algorithm,

```
WiFi ClientespClient;
PubSub Clientclient (espClient);
longlastMsg = 0;
charmsg[50];
String msg1;
//int value = 0;
#define relay  D1
#define relay1 D4
#define relay2  D2
#define relay3  D3
#define trigPin D5
#define echoPin D6
#define buzzer D7
floatduration,distance;
voidsetup_wifi() {
if(payload[0]=='1')
  {
digitalWrite(relay,HIGH);
//    digitalWrite(relay1,LOW);
//    digitalWrite(relay2,LOW);
//    digitalWrite(relay3,LOW);
  }
else  if(payload[0]=='2')
  {
digitalWrite(relay,LOW);
//  digitalWrite(relay1,LOW);
//  digitalWrite(relay2,LOW);
//  digitalWrite(relay3,LOW);
  }
```

System function is when the desired command is provided by admin through the MQTT dashboard or HiFi App as shown in Fig 6. The HiFi App sends the message to the cloud and the HiFi receives the message and verifies the transmitter and passes the data to the IoT, home automation network and switches on the allocated light and vice the other way around.If the HiFi detects a DDoS attack then that collection of data is stored within the HiFi system in a separate folder and blocks its further movement towards the IoT device along with a buzzer alarm to alert the administrator of the attack. This is made possible by programming the Raspberry pi 3B+ in using the Jet Brains PyCharm Community Version 2018.1.3 which is shown in Fig 7 and Fig 8 shows the main activity code for connecting the HiFi with the IoT devicesRaspberry pi 3B+ is designed to function as a server, as well as creating separate files within the Raspberry (pi 3B+). One folder will display the real data from the IoT devices and the other will store the unauthorized data from the cloud. The second IoT device is the temperature detection system, where the temperature sensor DHT11 is located. Fig 2.is connected and the room temperature is measured, the output can be seen via the HiFiApp Fig 6. The software is built using Android studio, which allows the IoT devices to be controlled. Using the Software, the user can provide approved data and read the temperature from the App. The Node MCU program for DHT11 Temperature sensor is Fig 9 and the picture of final output when different relays are turned On and Off are shown in Fig 11.

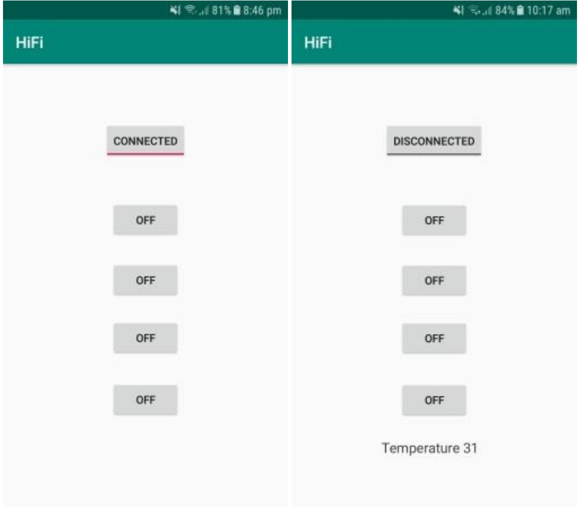


Fig 6: HiFi App disconnected mode and connected mode with room temperature

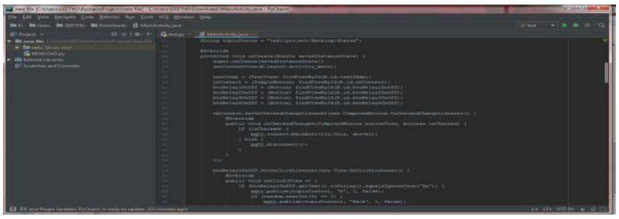


Fig 7: Jet Brains PyCharmCommunity Edition

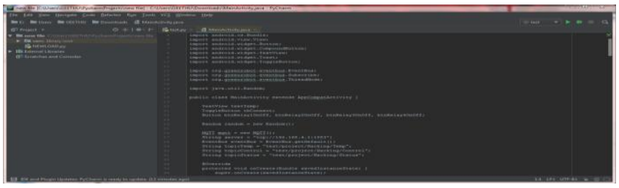
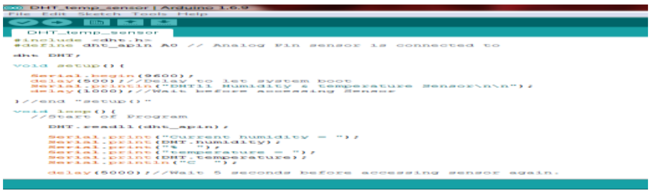


Fig 8: Main activity code for the seperation of folders in Raspberry pi 3B + 2018.1.3,code for connecting the HiFi with the IoT devices



```
#include <dht.h>
#define dht_apin A0 // Analog Pin sensor is connected to
dht DHT;
void setup(){
  Serial.begin(9600);
  delay(500);//Delay to let system boot
  Serial.println("DHT11 Humidity & temperature Sensor\n\n");
  delay(1000);//Wait before accessing Sensor
}//end "setup()"
void loop(){
  //Start of Program
    DHT.read11(dht_apin);
    Serial.print("Current humidity = ");
    Serial.print(DHT.humidity);
    Serial.print("%  ");
    Serial.print("temperature = ");
    Serial.print(DHT.temperature);
    Serial.println("C  ");
    delay(5000);//Wait 5 seconds before accessing sensor again.
```

Fig 9: Node MCU program for DHT11 Temperature sensor

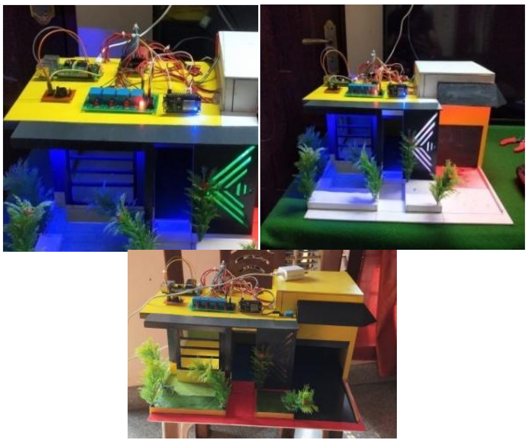


Fig 10: Output Of Home Automation System When One Relay Is Turned On and Off

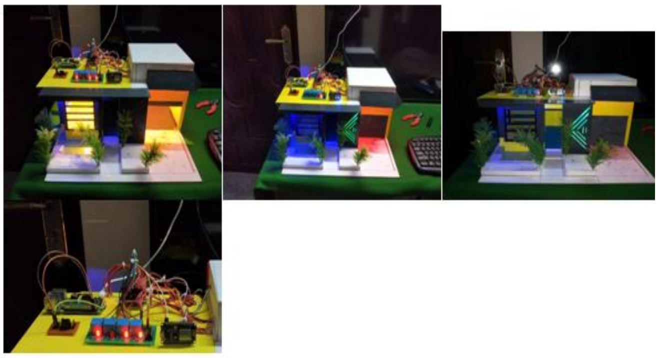


Fig 11: Output when different relays are turned ON and OFF

V. CONCLUSION

Most of the current solutions tackle software-level security problems, such as Stack Guard, Point Guard, and HS Defender but with the additional code, they also cause high performance overhead. Therefore, using an unique hardware unit to detect buffer overflow attacks does not create extra performance losses to the original execution of the program, and can also accomplish speedy detection (reasonable design can create real-time identification), such research is very important.. A very unique new approach has been introduced to prevent hacking and is the most reliable solution to prevent IoT devices from hacking attacks. It is compact and it is cost-effective. This product has the main advantage that it is a hardware device for IoT security and management. Like hardware devices with apps, they are less vulnerable to attack. HiFi system will guarantee a much safer IoT setting. Current research is done by wired communication concentrating only on local area, but more IoT devices can be linked together via wireless in the future.

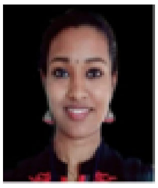
ACKNOWLEDGMENT

We would like to show our gratitude to Dr. Arun Surendran , Principal and Strategic Director of Trinity college of Engineering, Trivandrum, Kerala for sharing his pearls of wisdom with us during the course of the research work. His views on the emerging technologies made us to think more deeply into the roots of existing works.

REFERENCES

1. Mobility Report, November,2016
2. Abdulhafis Abdulazeez Osuwa, Esosa Blessing Ekhoragbon, Lai Tian Fat, "Application of artificial intelligence in Internet of Things," International Conference on Computational Intelligence and Communication Networks, 2017
3. Gartner, "Forecast: IoT Security, Worldwide",2016.
4. Bin Xu, Weike Wang, QiangHao, Zhun Zhang, PeiDu, Tongsheng Xia, Hongge Li, Xiang Wang, "A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device", IEEE Access, 2018
5. N. Mukrimah, A. Amiza, Y. Naimah and B. L. Ong, "Internet Of Things(IoT) : Taxonomy of Security Attacks," in International Conference on Electronic Design(ICED), Phuket., 2016.
6. Se-Ra Oh, Young-Gab Kim , "Development of IoT security component for interoperability," International Computer Engineering Conference (ICENCO), IEEE, 2017.
7. Ahmet Efe, Esra Akosoz, Neslihan Hanecioglu, Şeyma Nur Yalman ,"Smart Security of IoT Against DDOS Attacks", International Journal of Innovative Engineering Applications, vol.2, 2018, pp. 35-43.
8. Anton O. Prokofiev, Yulia S. Smirnova, Vasiliy A. Surov, "A method to detect Internet of Things botnets," Young Researchers in Electrical and Electronic Engineering (EIConRus) IEEE Conference of Russian, 2018, pp. 105-108.
9. Cusack B, &Tian, Z , "Evaluating IP surveillance camera vulnerabilities," The Proceedings of Australian Information Security Management Conference,2017, pp.25-32.
10. C. Cowan, S. Beattie, J. Johansen, and P. Wagle,"PointGuard: Protecting pointers from buffer overflow vulnerabilities, " Proc. USENIX Security Symp, 2003, pp. 91- 104.
11. Shao, Zhili, Xue, Chun, Zhuge, Qingfeng, Meikang, Qiu, "Security Protection and Checking for Embedded System Integration against Buffer Overflow Attacks via Hardware/Software," IEEE transaction on computers, vol.55 (4), 2006, pp. 443-453.
12. https://wiki.dfrobot.com/DHT11_Temperature_and_Humidity_Sensor__SKU__DFR0067_

AUTHORS PROFILE



Bhadra Priya S. S. B.Tech graduate in Electronics and Communication Engineering from A P J Abdul Kalam Technological University (KTU). She is currently working as 'Project coordinator' at Green Valley International School. She is also been selected as the Innovator of 'Young Innovators Programme' 2018-2021, by the Kerala Development and Innovation Strategic Council (K-DISC). While in college she served as the CEO (Chief Executive officer – highest position served by a student), during the year of 2016 – 2019, in TRINITY- IEDC (Innovations and Entrepreneurship Development Cell), and got recognized with many awards in research, innovation and entrepreneurship field. 'DIGIZON JACKET' funded by Center for Disability studies and 'AGRIBOAT' funded by Kerala Startup Mission, are some among the funded projects she handled. Anything innovative will be her area of interest, but to make it short to three, Nano Technology, IOT and Networking.

Nishi S Das, received her Bachelor's degree in Electronics and Communication in 2006 and her Master's degree in Communication System in 2012 from Noorul Islam Center for Higher Education. She is currently working as Assistant Professor in Electronics and Communication Engineering Department at Trinity College of Engineering, Trivandrum, Kerala, India. She has 2 years of Industrial experience and 7 years of teaching experience. She is pursuing PhD in Noorul Islam Center for Higher Education..She has published several Scopus indexed journals. Her research interests are Medical Image Processing, Applied Electromagnetic Theory, Information Theory and Coding.