CYBER SECURITY IN POWER SYSTEMS

TEAM 7 REPORT
EEPC-18
POWER SYSTEM ANALYSIS

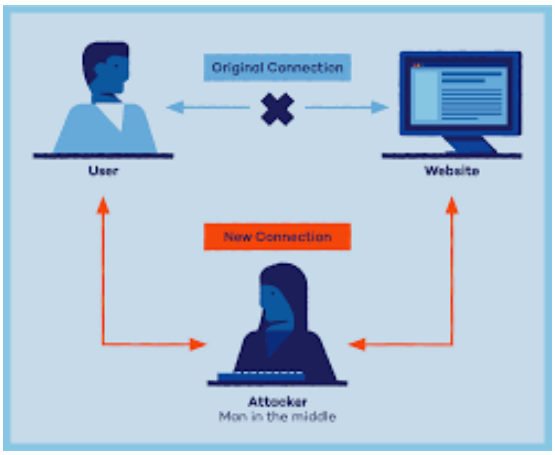
FACULTY –
DR.M. JAYA BHARATHA REDDY

AIM:

To create and detect a cyber-attack in the power system.

THEORY:

MAN IN THE MIDDLE ATTACK:



A **man-in-the-middle (MITM) attack** is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway**.**

A MITM attack Analogy:

A mailman opens your bank statement, writes down your account details, reseals the envelope, and delivers it to your door.

There are two stages for the MITM attack.

- Interception
- Decryption

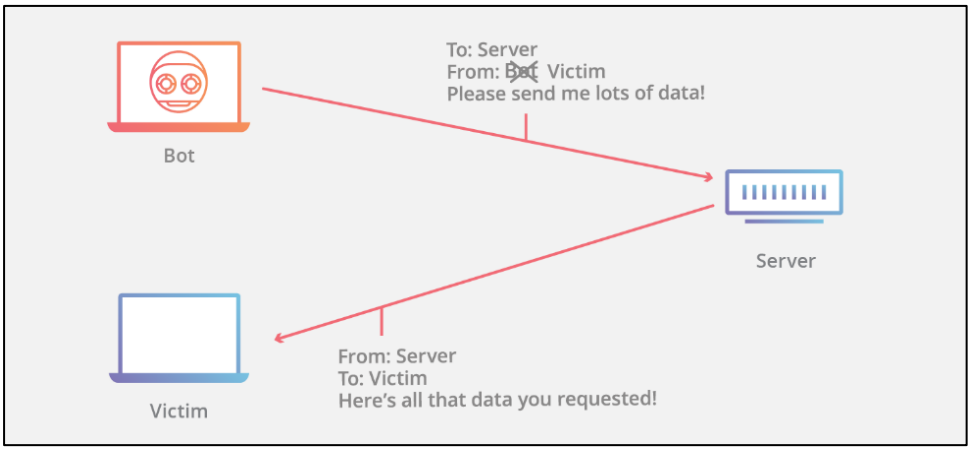
Interception Approach:

Intercepting user traffic through the attacker's network before it reaches its intended destination.

Several methods exist to achieve this:

- IP spoofing: involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.

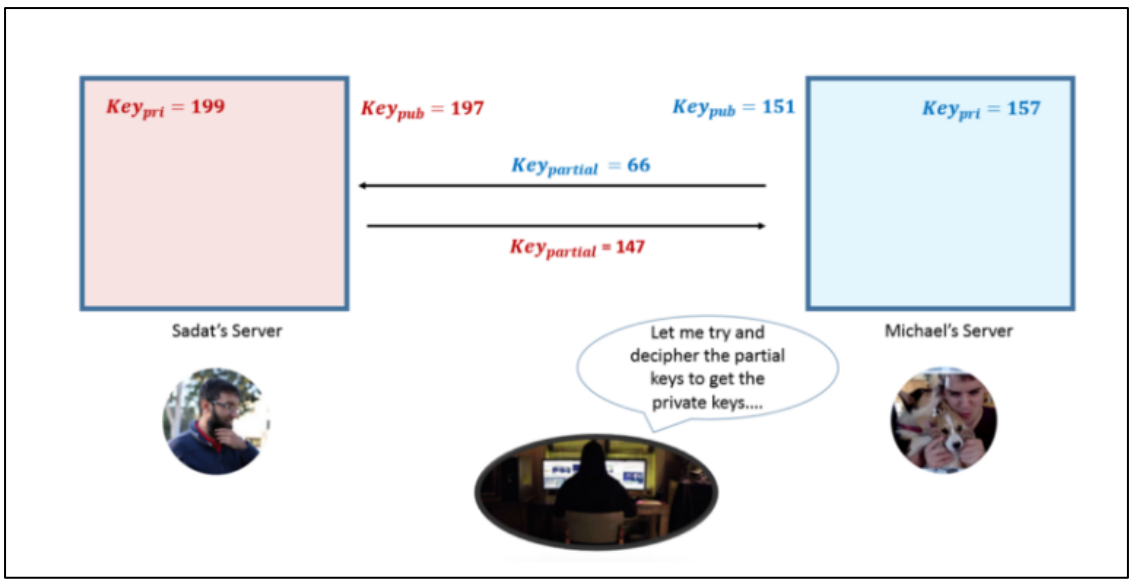
- *ARP spoofing: linking an attacker's MAC address with the IP address of a legitimate user on a local area network using fake ARP messages. As a result, data sent by the user to the host IP address is transmitted to the attacker.



KEY EXCHANGE:

Diffie–Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel.

- A key in cryptography is a piece of information. Usually, a string of numbers or letters is stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.
- Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. Cryptography is generally about constructing and analyzing protocols that prevent third parties or the public from reading private messages.



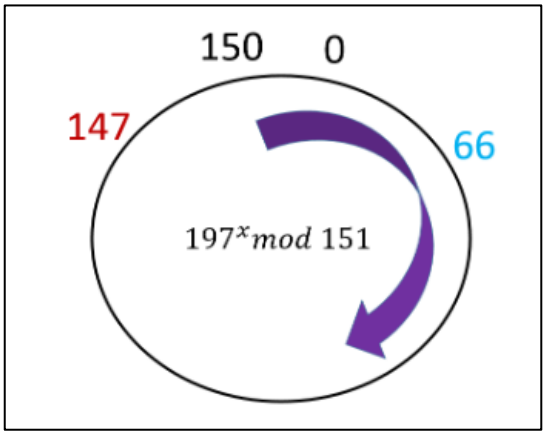
PARTIAL KEY GENERATION:

$$Key_{partial} = Key_{pub}{}^{Key_{pri}} \, mod \, Key_{pub}$$

FULL KEY GENERATION:

$$Key_{full} = Key_{partial}{}^{Key_{pri}} \, mod \, Key_{pub}$$
$$= 66^{199} mod \, 151$$
$$= 75$$

INFINITE POSSIBILITIES OF PRIMARY KEY (X):



SUCCESSFUL TRANSMISSION OF FULL KEYS:

$$Key_{full} = Key_{partial}{}^{Key_{pri}} \, mod \, Key_{pub}$$
$$= 66^{199} mod \, 151$$
$$= 75$$

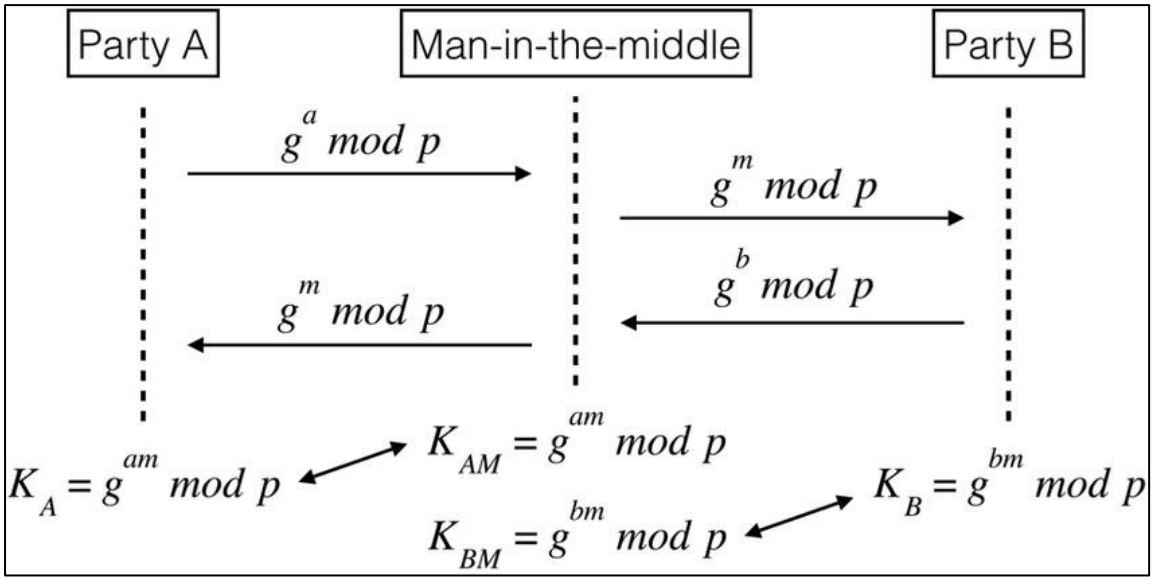
$$Key_{full} = Key_{partial}{}^{Key_{pri}} \, mod \, Key_{pub}$$
$$= 147^{157} mod \, 151$$
$$= 75$$

THE ENCRYPTION AND DECRYPTION OF FULL KEYS:

Encryption: converts the message into integers and adds the value of the key and then converts back to cipher messages.

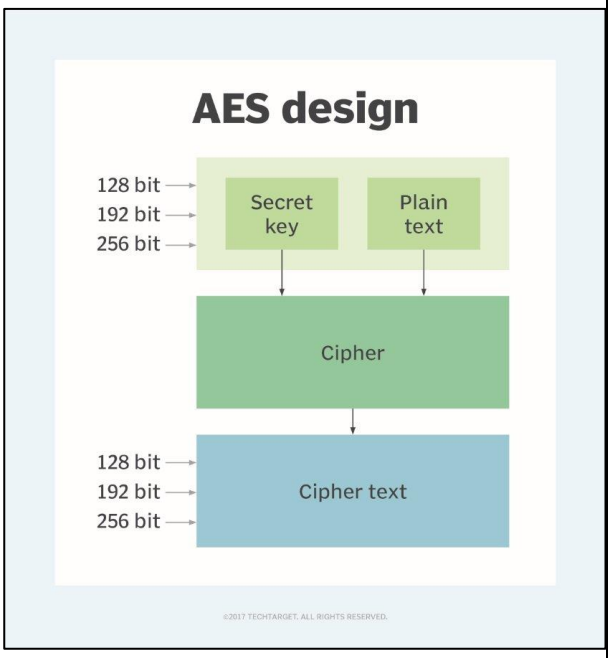
Decryption: converts the cipher messages into integers and subtracts the key value, and converts back to the original message.

MAN-IN-THE-MIDDLE ATTACK(MITM):



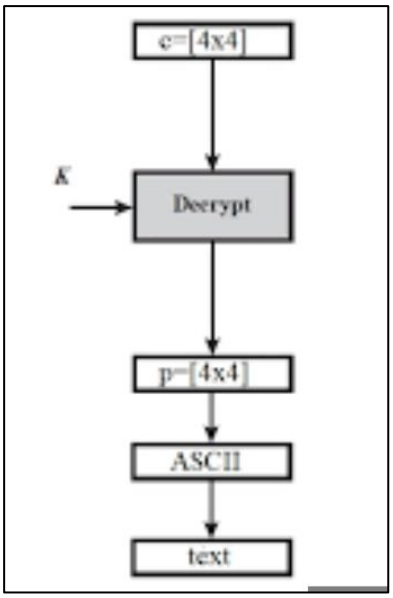
ADVANCED ENCRYPTION STANDARD:

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

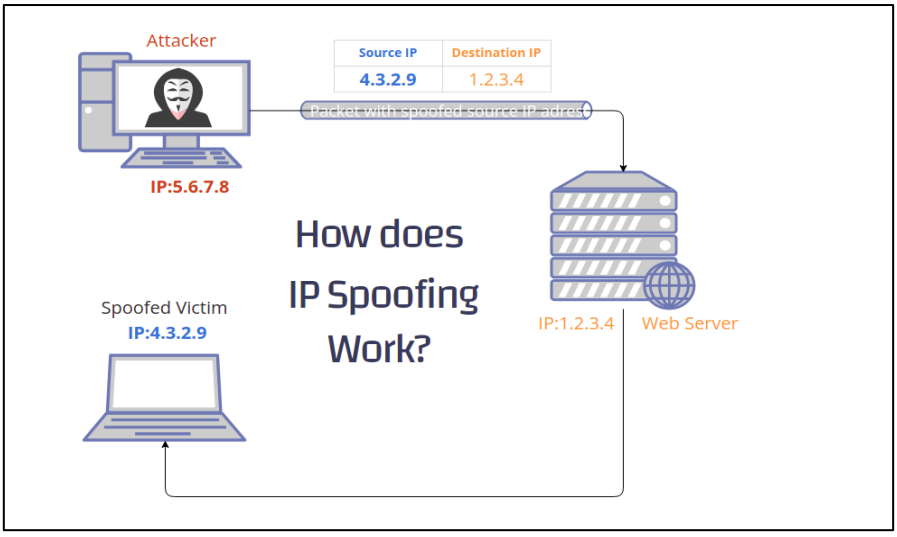


ENCRYPTION AND DECRYPTION:

The stages in the rounds can be easily undone as these stages have an opposite to it, which, when performed, reverts the changes. Every 128 blocks go through the 10,12 or 14 rounds, depending on the key size



IP Spoofing:

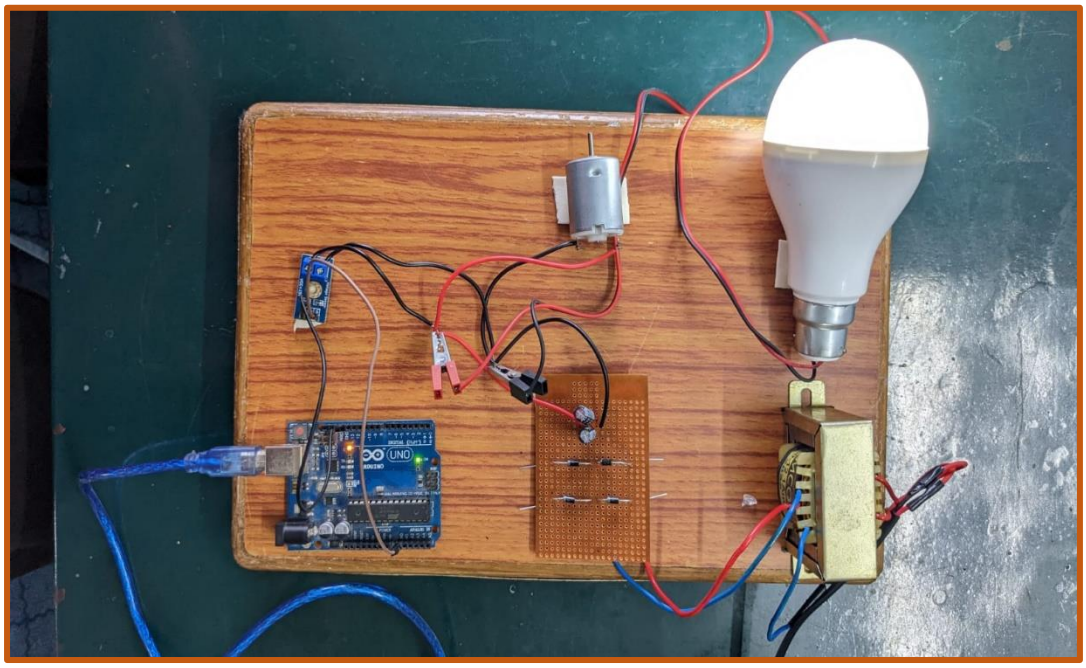


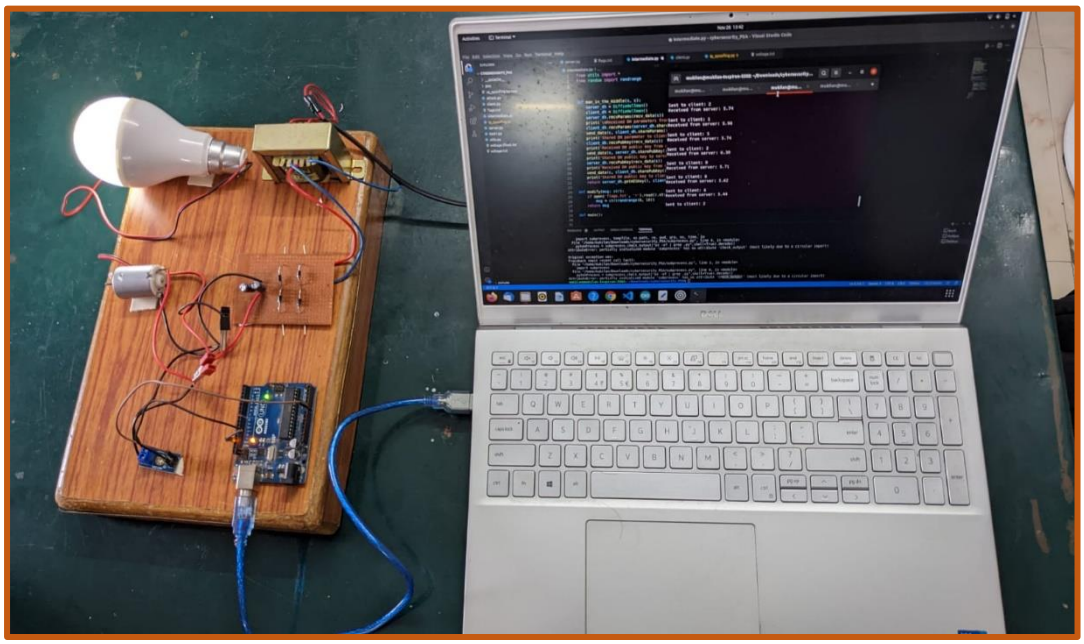
The attacker hacks into the system by pretending as a node in the system and accessing and requesting data from the web server. If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed. Relatedly, if the receiver wants to respond to the return address, their response package will go somewhere other than to the real sender.

COMPONENTS USED

- Step Down Transformer - 230/12 V , 1A
- Isolation Transformer - 12/12 V, 1A
- Arduino UNO
- Voltage Sensor EC-2173
- Rectifier Circuit (4*Diodes 1N4007- 1A, Capacitor 2*100 µF)
- DC Motor 12V
- DC bulb 12V, 9W

HARDWARE:





CODE :

ARDUINO CODE:

```
//Reading Analog Data
const int voltageSensor = A0;

float vOUT = 0.0;
float vIN = 0.0;
float R1 = 30000.0;
float R2 = 7500.0;
int value = 0;

void setup()
{
Serial.begin(9600);
}

void loop()
{


  value = analogRead(voltageSensor);
  vOUT = (value * 5.0) / 1024.0;
  vIN = vOUT / (R2/(R1+R2));
  Serial.println(vIN);
  delay(1500);


}
```

SERVER:

```
def main():

    server_sock = server_socket('localhost', 3000)
    client_sock, _ = server_sock.accept()
    aes = on_new_connect(client_sock)


    while True:
        msg= serial_port.readline().decode('ascii')
        communicate(client_sock, aes, msg.encode())
        print(f'Sent: {msg}')
        sleep(1)
```

INTERMEDIATE (ATTACKER):

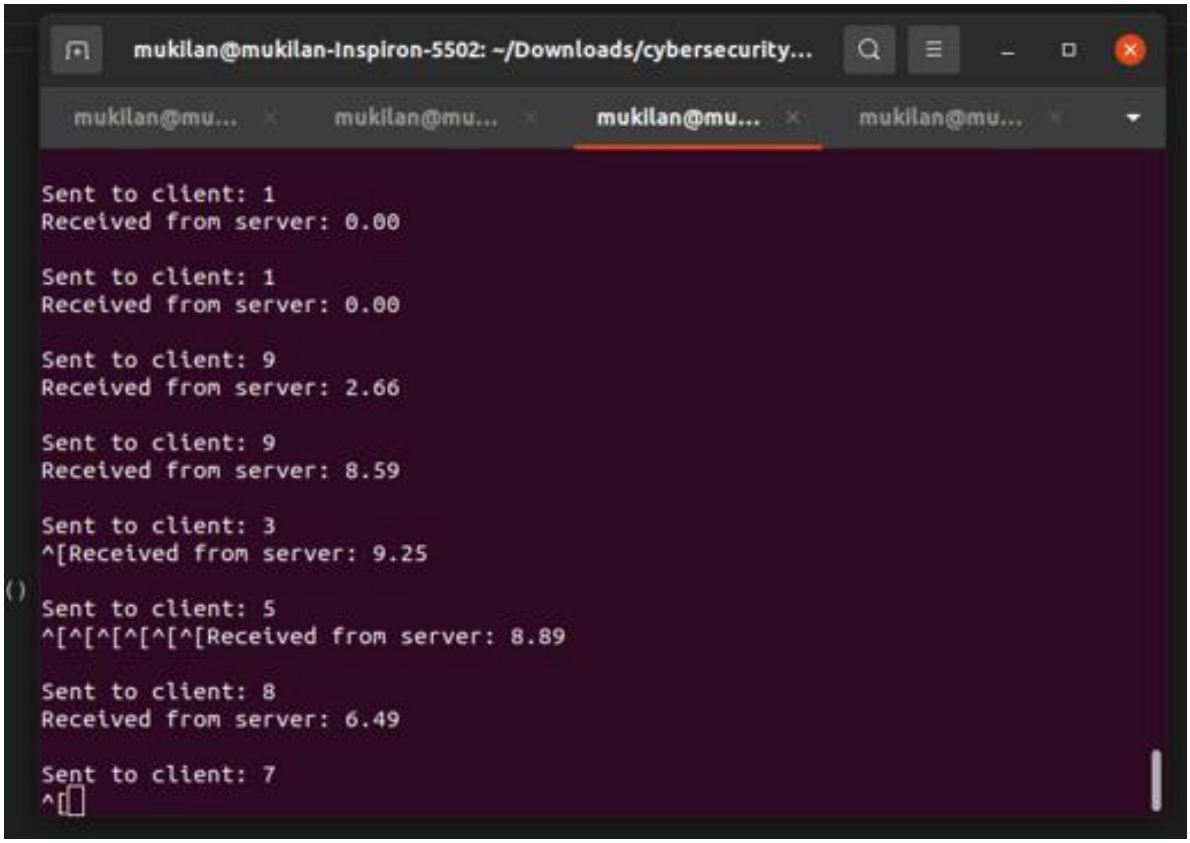
```
def main():


    listen_sock = server_socket('localhost', 4000)
    client_sock, _ = listen_sock.accept()
    s = socket.socket()
    s.connect(('localhost', 3000))

    server_aes, client_aes = man_in_the_middle(s, client_sock)

    try:
        while True:

            if open('flags.txt', 'r').read().strip() == '1':

                msg = communicate(s, server_aes).decode()
                print(f'Received from server: {msg}')
                msg = modify(msg)
                communicate(client_sock, client_aes, msg.encode())
                print(f'Sent to client: {msg}')

            elif open('flags.txt', 'r').read().strip() == '0':

                msg = communicate(s, server_aes).decode()
                msg = modify(msg)
                communicate(client_sock, client_aes, msg.encode())
```

CLIENT:

```
def main():

    s = socket.socket()
    s.connect(('localhost', 4000))
    aes = on_new_connect(s)

    try:
        while True:
            msg = communicate(s, aes).decode()
            print(f'Received: {msg}')

    except socket.error:
        pass
    except Exception as e:
        print(str(e))

    s.close()

if __name__ == '__main__':
    main()
```

EXPERIMENTAL RESULTS:

During the Attack:



TEAM MEMBERS:

1. PRANAV KRISHNA 107120134
2. MUKILAN-107120074
3. VIKASH-107120124
4. KISHORE-107120064
5. MANISH-107120068
6. AYUSH-107120024
7. SHIVAM-107120112
8. GANESH-107120076