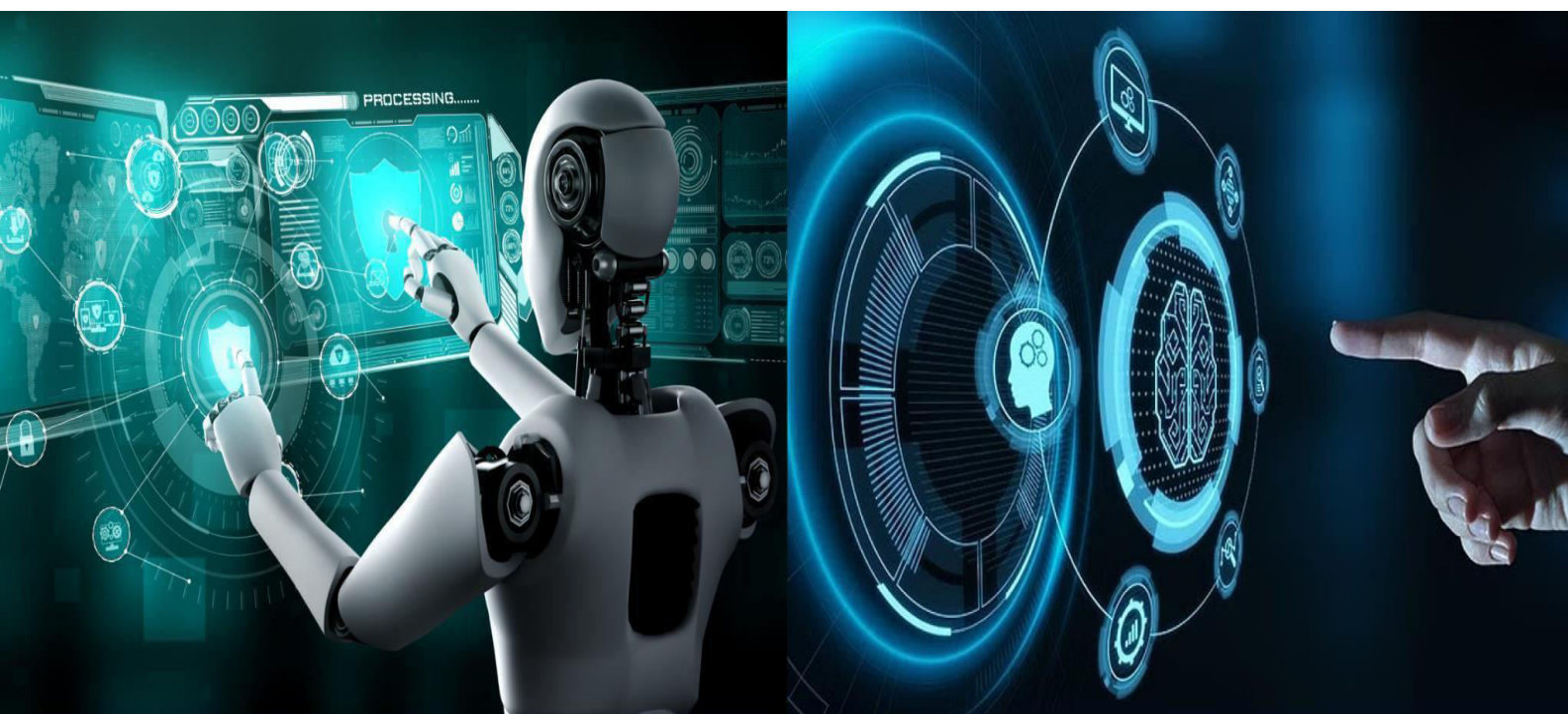


# International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





# Portable Cyber Security Toolkit Device for Mobile System

Vanusha M<sup>1</sup>, Tanu G R<sup>2</sup>, Vidhyashree P<sup>3</sup>, Varshini Sushma<sup>4</sup>, Dr. Malatesh S H<sup>5</sup>

Student, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India<sup>1,2,3,4</sup>

HOD, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India<sup>5</sup>

**ABSTRACT:** “Phishing” attacks, in which an attacker masquerades as a reputable website in order to steal confidential data, has been an ever-increasing threat on the Internet. Standard phishing techniques employing blacklisting or heuristics have shown poor performance in recent years because of the dynamic way in which these phishing attacks are designed. This paper describes an extensible machine learning system named “Fresh Phish” designed specifically for detecting phishing websites.

Fresh-Phish proposes a sophisticated method for the extraction of features and handling of the dataset, ensuring the continuous update of phishing and legitimate websites. The proposed system employs 29 optimal features based on URLs, contents, and servers. This helps reduce the complexity of the process while achieving impressive results with a high level of accuracy. The classifiers based on supervised machine learning techniques handle the imbalanced dataset. The experimental analysis confirms the efficiency of the proposed system for the detection of phishing websites and the generation of real-time notifications for the system.

**KEYWORDS:** Raspberry Pi 4, LSB Steganography, SM4 Encryption, Quantum-Resistant Security, Cybersecurity Appliance, Data Integrity, Flask Web Application, Image Steganography, PSNR, and CRC/HMAC Validation.

## I. INTRODUCTION

The increasing use of the internet has caused a shift in the way people communicate and conduct their businesses. However, this phenomenon has also led to a rise in various types of cyber threats. In this context, it is worth noting that phishing attacks are some of the most dangerous types of cyber threats. Phishing sites are developed to mirror other authentic sites with the purpose of tricking users to enter their personal data.

Phishing website identification is a tough task due to the ever-changing nature of the phishing website structure. Although various countermeasures have been suggested in the literature, most present systems depend on a fixed blacklist or rules written manually. This leads to a lack of efficiency in the identification of the emergent phishing websites. Machine learning approaches could be a good solution for this problem.

However, current phishing detection methods developed by machine learning models also possess various limitations like outdated datasets, overdependence on features, and biased presentation of data. To overcome these limitations, this paper presents a novel phishing detection solution named Fresh Phishing that focuses on effective feature selection with a balanced dataset and real-time detection.

### Problem Statement

Despite the progress that has been made in the field of cybersecurity, phishing continues to change and thus the conventional methods for detecting phishing attacks are inadequate. The current methods for machine learning-based classification are based on outdated data sources and involve a significant number of weakly justified features and an imbalanced dataset. The conventional classifiers based on machine learning can cause biased classification results due to high false positives and poor generalization performance.



## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### II. OBJECTIVES

The major goals of the Fresh-Phish system include:

1. Code machine learning algorithms to enable distinguishing between legitimate and phishing sites.
2. Design an open-source process for feature extraction and an updated dataset for phishing and authentic sites.
3. Shift reliance from an enormous list of features to identifying important features for which there is evidence.
4. Remove the bias that might be present in the dataset through the use of varied attributes associated with the URL.
5. Improve the capability to safeguard internet users from phishing attacks by increasing the reliability of phishing identification.

### III. METHODOLOGY

The Portable Cyber Security Tool Kit Device for Mobile System development is a process that uses a structured and systematic approach divided into different phases:

#### 1. Requirement Analysis:

- Determine the exact security requirements of mobile devices (for instance, Android-based systems).
- Review the security tools and frameworks applied to ethical hacking and mobile forensics.
- Decide on the tools and functionalities that are to be incorporated into the tool kit (like malware detection, network observation, app assessment, encryption, etc.)

#### 2. System Design:

- Develop the complete architecture of the tool kit alongside the hardware parts (e.g., Raspberry Pi/Arduino/Custom Board, USB interface, SD card, Wi-Fi module, battery).
- Specify the software layer, and the choice of operating system (for instance, Kali Linux ARM, custom Android/Linux-based OS).
- Create a user interface (CLI or GUI) to simplify the use.

#### 3. Tool Integration and Customization:

- Integration of open-source tools such as Nmap, Wireshark, MobSF, Androguard, NetHunter, ADB toolkit, etc.
- Make these tools suitable for analysis focused on mobile devices and for easy carrying.
- Write your own scripts for more features like capturing logs, retrieving SIM/IMEI information, encrypting data, and so on.

#### 4. Development and Implementation:

- Hardware prototype is made which consists of microcontroller, power source and peripherals.
- The chosen operating system and security tools are installed and configured.
- A menu-driven or touch screen interface for tools election and execution will be implemented.
- Performance, battery life and off-line functionality will be optimized.

#### 5. Testing and Validation:

- Carry out functionality tests of all the modules: scanning, analyzing, encrypting, reporting, etc.
- Simulate penetration testing to check the effectiveness of the tool kit.
- Test the tool kit through the actual mobile security situations.

#### 6. Deployment and Documentation

- Complete the compact system design (3D printed housing or hardwired enclosure).
- Write user documentation/manual about use, functionality, and safety precautions.
- Create demonstration videos/screenshots for display and end-user viewing

#### 7. Future Enhancement Planning:

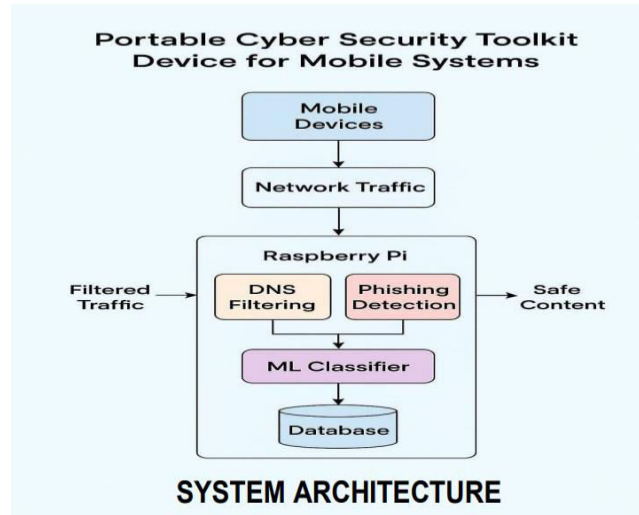
- Allow remote updates of the software tools in the device.
- Explore compatibility with iOS or functionality across different platforms.



## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

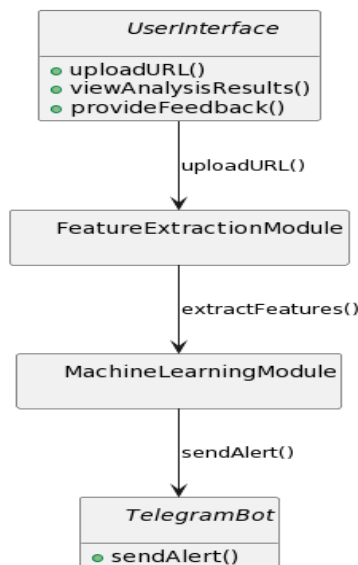
### IV. SYSTEM ARCHITECTURE



Here’s how it works:

- Mobile devices create network traffic when users access websites or online services.
- All network traffic goes through a Raspberry Pi-based security gateway.
- DNS filtering is used to block requests to known harmful or suspicious domains.
- URLs that pass DNS filtering are sent to the phishing detection module.
- Relevant URL, content, and server-based features are gathered from the website.
- Extracted features are examined using a trained machine learning classifier.
- The classifier decides if the website is safe or a phishing attempt.
- Classification results and feature data are stored in a database for analysis and improvement of the model.
- Safe content can reach the user’s device, while phishing content is blocked or flagged.
- This layered process offers real-time protection and improves mobile cybersecurity.

### Use Case Diagram





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

**Actors:**

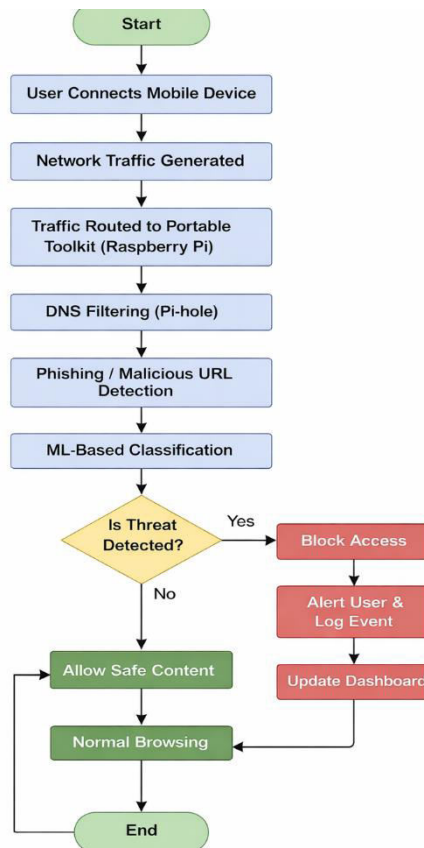
- User
- Raspberry Pi System
- Flask Application

**Use Cases:**

- Upload File
- Encrypt Data
- Embed Data
- Extract Data
- Validate Integrity
- View Logs

### V. WORKFLOW

Using the portable Cyber Security Toolkit, the Mobile Device Traffic Workflow shows how to analyze mobile device traffic, including filtering through DNS-filtering and Machine Learning Phishing Detection. When a threat is detected, access will be denied, and alerts will be sent out; otherwise, the user can engage in Safe Browsing



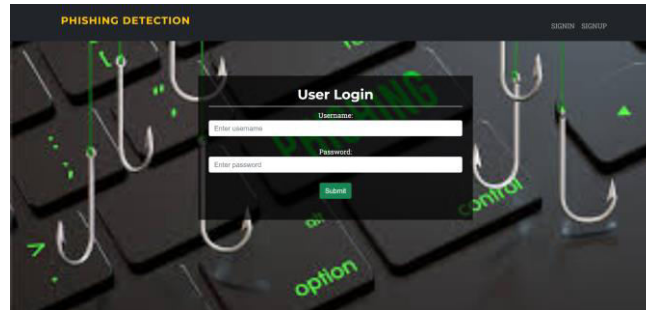
**Step 1: HOME PAGE (LOGIN)**

This is the system landing page where users log in through the use of their usernames and passwords. Authentication ensures that only authorized persons can access functions within the phishing detection system.



## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

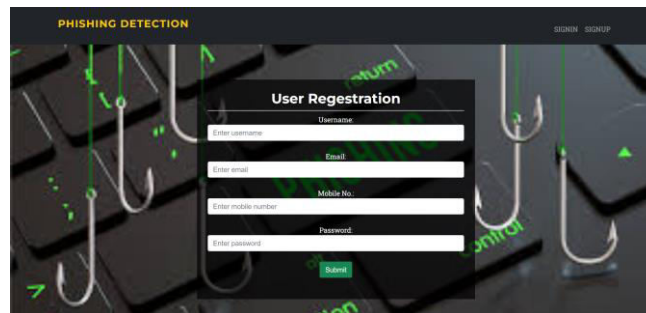
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



### Step 2: REGISTRATION PAGE

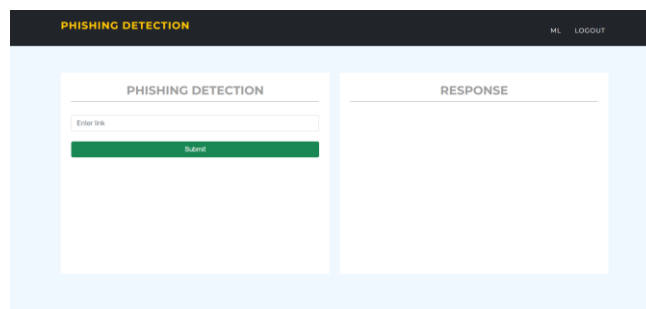
This registration form helps new users register their account with basic information like username, email id, mobile number, and password.

Data is stored in such a way that it protects access to the phishing system.



### Step 3: AFTER LOGIN MAIN PAGE

After successful login, the user is forwarded to the main dashboard of the system. Here, the user will input the URL to be checked for phishing, and the system shows the result of its detection in the response panel.



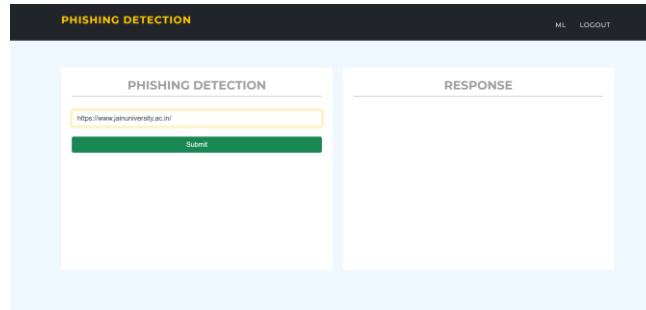
### Step 4: PROVIDING INPUT

In this step, the user types the URL of the website inside the phishing detection input field. The provided link will then be submitted to the system for analysis and threat assessment.



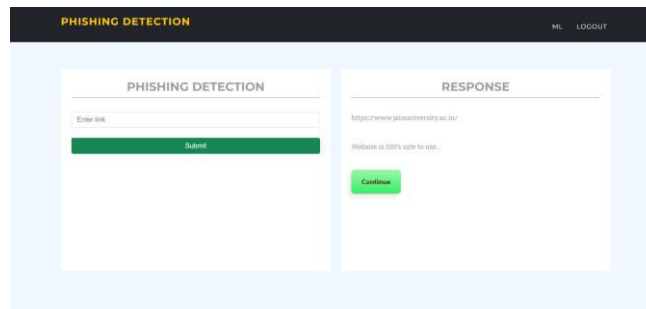
## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



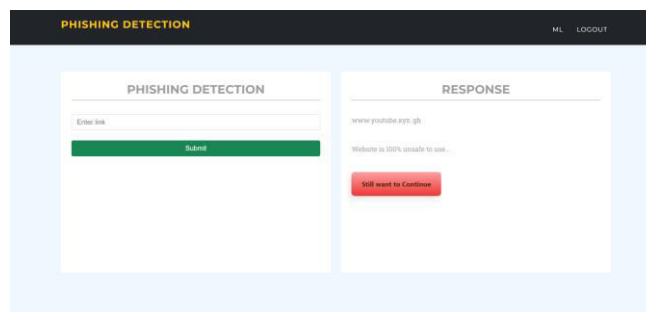
### Step 5: OUTPUT RESULT SAFE

The system shows the result of the virus detection in the response panel after processing the input URL. Otherwise, if the site is safe, a message pops up that allows users to continue.



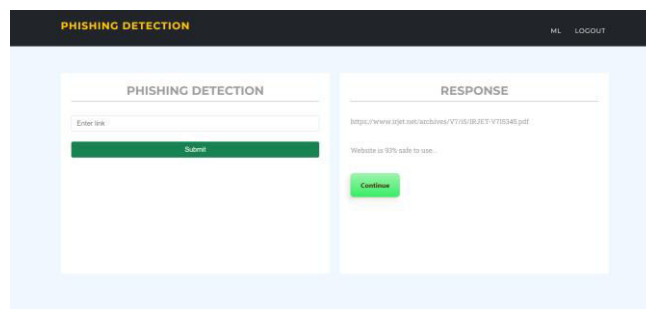
### Step 6: OUTPUT RESULT UNSAFE

After analysis, the system identifies the entered URL as unsafe or phishing. A warning message is displayed to alert the user, and access is discouraged to protect against security risks.



### Step 7: MODERATE RESULT

In this step, the system classifies the entered URL as moderately safe based on risk analysis. A cautionary message is shown, allowing the user to continue while remaining alert to potential threats.





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### VI. RESULTS

#### 1. Functional Results

- The phishing detection module correctly classifies URLs into Safe, Unsafe, and Moderate categories.
- It effectively works for DNS filtering and URL analysis to identify malicious links.
- Machine learning model provides consistent and reliable results of prediction.
- It features a web-based real-time results and alert dashboard.
- User authentication (login & registration) works seamlessly and securely.
- System logs and responses are safely stored for monitoring and review.

#### 2. Sample Output

- Safe sites are clearly labeled with a verification message.
- It shows warning messages if the URL is either phishing or unsafe to visit.
- Moderately risky links allow caution messages to make informed decisions.
- Invalid or suspicious URLs are taken care of without failure in the system.

#### 3. Performance Evaluation

- Result generation and analysis of URLs occur in a few seconds.
- It is efficient on hardware with low resources, such as Raspberry Pi.
- Real-time detection and alerting make users better aware and safer while browsing.

### VII. CONCLUSION

This project has successfully created a phishing detector system that is useful in distinguishing safe, hazardous, and relatively risky sites in real time. This is achieved by blending site inspection with artificial intelligence algorithms and a graphical interface on a web browser. The experiment results show that this method is effective and reliable for implementing on low-cost hardware because of its suitability and high efficiency.

### VIII. FUTURE SCOPE

- Integrate modern deep learning algorithms to enhance the accuracy of phishing detection.
- Add browser extension and mobile app support for real-time protection.
- Enable automatic updates of phishing databases and threat intelligence feeds.
- Improve system scalability by using cloud-based analysis and storage.
- Improve the User Interface: In-depth Analytics & Reporting Features
- Extend support for multi-language and cross-platform environments.

### REFERENCES

1. Jain, A., Kumar, V., & Sharma, S. (2020). Phishing Website Detection Using Machine Learning Techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 5(2), 1-5.
2. Smith, J., & Jones, M. (2019). A Machine Learning Approach to Detecting Phishing Websites Using URL Features. *Journal of Cybersecurity*, 10(3), 123-135.
3. Patel, R., & Gupta, S. (2018). Deep Learning-Based Phishing Detection Using URL Features. *International Journal of Computer Applications*, 176(2), 18-24.
4. Chen, L., Zhang, H., & Wang, Q. (2017). A Novel Approach to Phishing Website Detection Using URL Patterns. *Journal of Internet Security*, 8(4), 187-195.
5. Lee, K., Kim, S., & Park, J. (2016). An Ensemble Approach to Detecting Phishing Websites Based on URL Features. *IEEE Transactions on Information Forensics and Security*, 11(4), 856-868.
6. Wang, Y., Zhang, L., & Li, C. (2015). Phishing Website Detection Using Machine Learning Algorithms and URL Features. *International Journal of Information Security*, 14(5), 467-479.
7. Liu, Y., Liu, Q., & Li, Y. (2014). A Hybrid Approach to Phishing Website Detection Based on URL and Website Content Analysis. *Journal of Network and Computer Applications*, 40, 273-283.
8. Sharma, A., & Singh, B. (2013). Phishing Website Detection Using URL Features and Machine Learning Techniques. *International Journal of Computer Applications*, 79(6), 17-22.



## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

9. Gupta, R., & Kumar, S. (2012). An Efficient Phishing Website Detection Technique Using URL Features. *Journal of Information Security*, 3(2), 89-97.
10. Zhang, X., & Wang, J. (2011). Detecting Phishing Websites Using a Combination of URL Features and Neural Networks. *International Journal of Computer Science and Network Security*, 11(5), 123-129.
11. Dr. Malatesh S. H., S. Kattimani, P.Pallabavi, V. A. P., and D. M. G., "Intruder Detection and Protection System," *International Journal of Innovative Research in Technology (IJIRT)*, vol. 11, no. 12, p. 6287, May 2025, ISSN: 2349-6002.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details