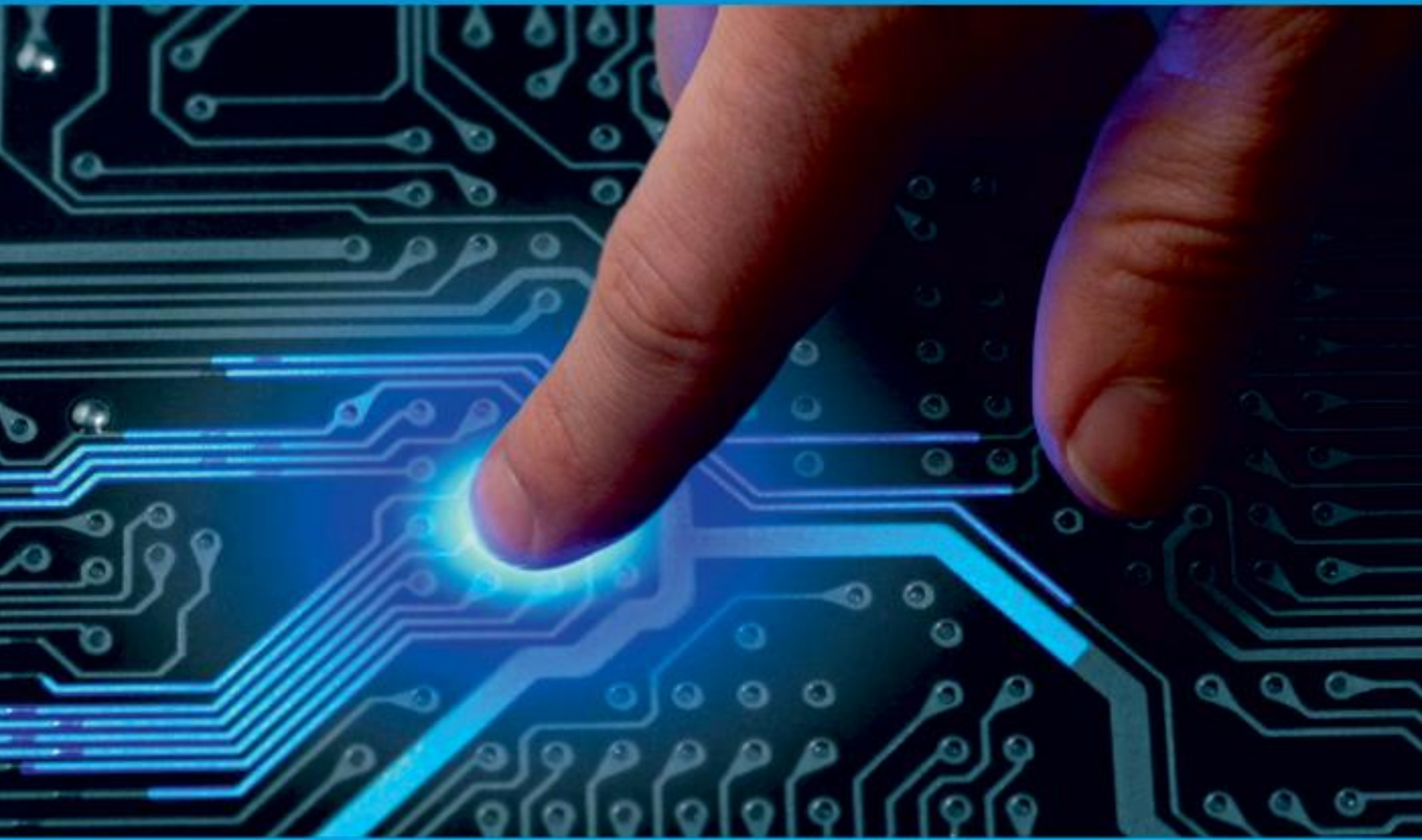
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

Classification and Mitigation of Cyber Attacks Using Machine Learning Approach

Pranav S[1], Sundaram S[2], Vignesh J[3], Saktheeswari R[4]

UG Student, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India[1,2,3]

Assistant Professor, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India[4]

ABSTRACT: Network cyberattacks are becoming a more serious threat in our hyperconnected world, affecting people, businesses, and governments with serious financial losses, data breaches, and operational disruptions. Effective defense mechanisms are desperately needed, as evidenced by the growing sophistication of attack vectors, which include malware, phishing, distributed denial-of-service (DDoS) attacks, and vulnerabilities in Internet of Things (IoT) devices like Slowloris and ARP poisoning. IoT device proliferation adds multiple points of entry for attackers and further complicates the security landscape. Conventional cybersecurity solutions are labor-intensive and prone to mistakes, and they frequently fall short. Our project employs a machine learning technique to categorize various cyber-attacks by utilizing a carefully selected dataset of behavioral characteristics and network traffic data. The model recognizes complex patterns among various attack types after being trained on labeled historical attack instances. Consistent updates and retraining with fresh data guarantee ongoing applicability, empowering cybersecurity teams to quickly recognize and address threats. By strengthening digital security frameworks, enhancing proactive cyberattack detection and mitigation, and enhancing network and IoT resilience, this research advances cybersecurity.

KEYWORDS: Cyber-attacks; Network security; Threat identification; IoT; Machine learning

I. Introduction

Managing the intricacies of our digitally connected world, identifying and preventing cyberattacks, protecting confidential information, maintaining privacy, and guaranteeing the integrity of vital infrastructure become critical priorities. Cyberattacks are a serious threat because so much personal, financial, and organizational information is now available online. They target data integrity and confidentiality in a number of industries. Furthermore, attacks on vital infrastructure—like power grids and healthcare systems—can cause major disruptions to services that are necessary for public safety.

Investigating the complexities of cyber-attack identification, we examine techniques like network traffic analysis and machine learning algorithms. Modern societies are interconnected, which increases the impact of these attacks and emphasizes how urgent it is to develop efficient detection and mitigation techniques. Cyberattacks also negatively impact consumer behavior and economic stability by undermining trust in the digital ecosystem, which goes beyond monetary losses and business interruptions. Data breaches and security incidents damage companies' and organizations' reputations, which has long-term effects on consumer trust and brand loyalty.

The cybersecurity environment is further complicated by the spread of Internet of Things (IoT) devices, which creates new avenues for cyberattacks. IoT attacks have the potential to take advantage of weaknesses in networked devices, endangering the security of vital infrastructure as well as people's privacy. Our project includes a number of modules, such as data preprocessing, feature selection, model selection and training, model evaluation, and deployment, in order to address these challenges. Through the use of these modules and a comprehensive strategy that includes stakeholder collaboration, technological advancements, and proactive defense tactics, our goal is to strengthen digital defenses and lessen the risks associated with malicious activity.

II. Related work

The authors of [1] examine resampling strategies for rectifying class imbalance in educational datasets, emphasizing the efficacy of hybrid approaches for very unbalanced data and ROS for somewhat imbalanced data. This highlights how important customized resampling methods are to improving predictive model performance in learning environments. An adaptive ensemble learning model for intrusion detection is shown in [4], demonstrating a notable increase in detection accuracy over conventional techniques. The study emphasizes how important data quality and ensemble learning are to improving detection performance. Moreover, [5] presents a ConvNet model for network intrusion detection that is based on transfer learning and shows exceptional performance in identifying both well-known and unknown threats. This demonstrates how transfer learning can be used to overcome intrusion detection problems caused by data deficiencies. Furthermore, Random Forest classifier outperforms other classifiers in terms of accuracy and execution time in [6]'s evaluation of classification algorithms for network intrusion detection. The study makes the case that successful intrusion detection requires excellent algorithms. In the meantime, [7] suggests a deep learning strategy based on RNN-IDS, demonstrating superior intrusion detection accuracy over conventional techniques. This highlights how effective deep learning methods are at improving intrusion detection skills. Furthermore, [8] presents a unique method for intrusion detection that combines deep neural networks and spectral clustering, exceeding conventional models in terms of detection accuracy. This demonstrates how combining deep learning and clustering approaches can enhance detection skills. Furthermore, [9] offers a mutual information-based feature selection technique for network intrusion detection that, when paired with LSSVM, exhibits better classification performance. The significance of feature selection in improving intrusion detection accuracy is emphasized in the study. Lastly, [10] suggests an IDS model that makes use of the RF classifier and achieves a high level of efficiency in identifying different kinds of assaults. This demonstrates how successful ensemble learning methods are at detecting intrusions. Together, these studies' creative methods, reliable algorithms, and practical strategies for dealing with data difficulties advance the field of intrusion detection.

III. PROPOSED METHODOLOGY

The proposed method is an integrated method that begins with data gathering, moves through phases of preprocessing and feature extraction, and ends with training a model to detect cyberattacks. The user interface is then a web application that gives users access to both historical and real-time data. The system receives live data inputs, processes them in real-time, and produces related live outputs so users may keep an eye on cyber dangers and take fast action. By streamlining data flow and analysis, this integrated strategy improves cybersecurity measures and gives stakeholders the authority to make informed decisions.

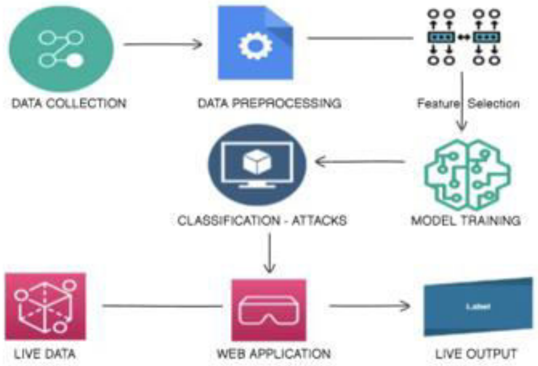


Fig.1. Architecture diagram

1.Data Collection:

Data is collected from a dataset that includes important network parameters such as energy consumption, service types, traffic volumes, packet sizes, TCP flags and attack identifiers that provide a comprehensive picture of network behavior. These parameters are necessary for machine learning models to effectively distinguish between normal and malicious activity. Analyzing these features improves cyber threat detection and mitigation.

2. Data Preprocessing:

- Perform data cleaning to handle missing values, outliers, and noise.
- Encode categorical variables into numerical format using techniques like label encoding and one-hot encoding.

- Apply data sampling techniques such as random sampling and SMOTE to manage imbalanced datasets.

3. Feature Extraction:

- Extract key attributes from network traffic data, including packet headers, flow statistics, and protocol usage patterns.
- Utilize techniques like SelectKBest to automatically retain the most relevant features for attack detection.

4. Model Selection and Training:

- Select machine learning algorithms suitable for cyber-attack classification, such as Gaussian Naive Bayes, AdaBoost, XGBoost, and Random Forest Classifier.
- Train the selected models using the preprocessed data to learn patterns and relationships within the dataset.

5. Model Evaluation:

- Assess the performance of trained models using metrics like accuracy, precision, recall, and F1-score.
- Visualize model performance using techniques like ROC curves and confusion matrices to gain insights into classification effectiveness.

6. Deployment:

- Integrate the trained models into a production environment for real-time monitoring of network traffic.
- Develop a user-friendly web application using Django framework to serve as the interface for users to interact with the system.
- Host the application on a production server, ensuring scalability, reliability, and security.
- Implement mechanisms for logging and auditing model predictions to facilitate post-deployment analysis and continuous improvement.

IV. SIMULATION RESULTS

The model was trained using four distinct algorithms: Random Forest Classifier, AdaBoost, XGBoost, and Gaussian Naïve Bayes. Figure 2 summarizes these classifiers' accuracy scores. With an accuracy of 99.82%, the Random Forest Classifier stands out for its outstanding performance. XGBoost comes very close behind with an accuracy of 97.28%. AdaBoost performs moderately with an accuracy of 38%, whereas Gaussian Naïve Bayes achieves a moderate 56.96% accuracy.

A more thorough grasp of each classifier's performance is possible thanks to its evaluation measures. The Gaussian Naïve Bayes Classifier's evaluation metrics are shown in Figure 3, which includes its precision, recall, and F1-score for each class. Comparably, Figure 4 shows the AdaBoost Classifier's assessment metrics, emphasizing its F1-score, precision, and recall despite its mediocre accuracy. Figure 5 further demonstrates the remarkable accuracy of the Random Forest Classifier by highlighting its precision, recall, and F1-score metrics, which highlight how well it can identify cyber threats.

Figure 6 showcases the user interface (UI) page, presenting the detected type of cyber-attack along with corresponding mitigation measures. In this figure, ARP poisoning, one of the classified attacks in this project, is detected. The displayed mitigation measures include implementing strong authentication and utilizing encryption protocols such as SSL/TLS to secure data in transit.

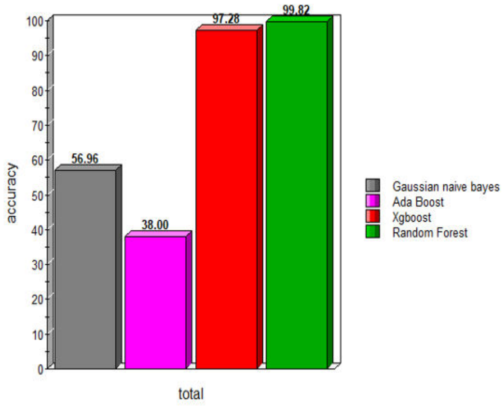
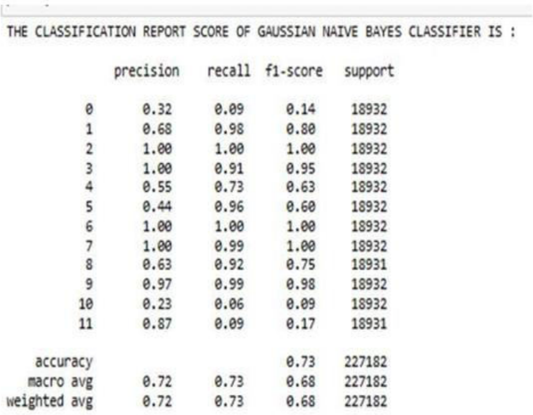


Fig.2. Accuracy scores of Classifier



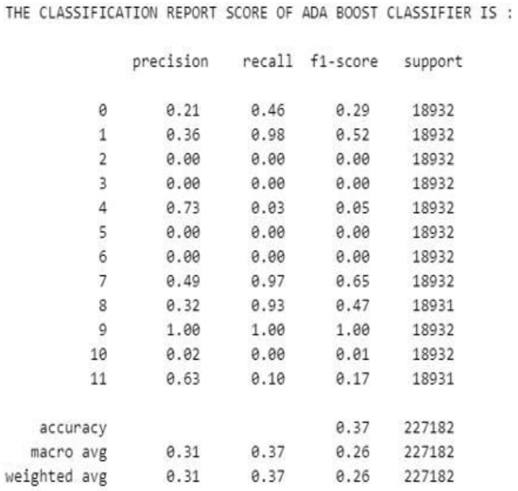
```
THE CLASSIFICATION REPORT SCORE OF GAUSSIAN NAIVE BAYES CLASSIFIER IS :

              precision    recall  f1-score   support

           0       0.32      0.09      0.14     18932
           1       0.68      0.98      0.80     18932
           2       1.00      1.00      1.00     18932
           3       1.00      0.91      0.95     18932
           4       0.55      0.73      0.63     18932
           5       0.44      0.96      0.60     18932
           6       1.00      1.00      1.00     18932
           7       1.00      0.99      1.00     18932
           8       0.63      0.92      0.75     18931
           9       0.97      0.99      0.98     18932
          10       0.23      0.06      0.09     18932
          11       0.87      0.09      0.17     18931

    accuracy                           0.73    227182
   macro avg       0.72      0.73      0.68    227182
weighted avg       0.72      0.73      0.68    227182
```

Fig. 3. Evaluation metrics for Gaussian Naives Bayes classifier



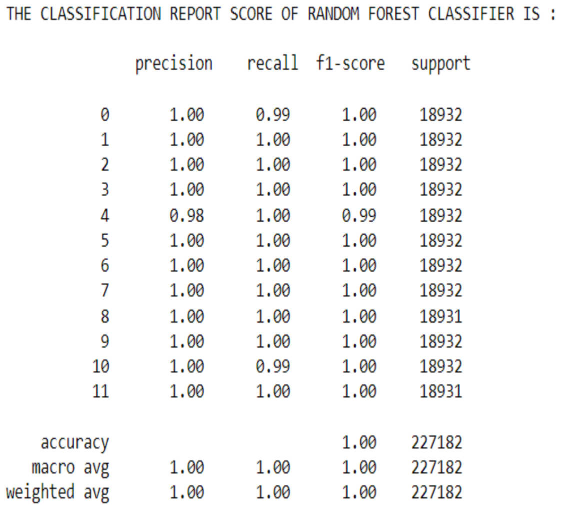
```
THE CLASSIFICATION REPORT SCORE OF ADA BOOST CLASSIFIER IS :

              precision    recall  f1-score   support

           0       0.21      0.46      0.29     18932
           1       0.36      0.98      0.52     18932
           2       0.00      0.00      0.00     18932
           3       0.00      0.00      0.00     18932
           4       0.73      0.03      0.05     18932
           5       0.00      0.00      0.00     18932
           6       0.00      0.00      0.00     18932
           7       0.49      0.97      0.65     18932
           8       0.32      0.93      0.47     18931
           9       1.00      1.00      1.00     18932
          10       0.02      0.00      0.01     18932
          11       0.63      0.10      0.17     18931

    accuracy                           0.37    227182
   macro avg       0.31      0.37      0.26    227182
weighted avg       0.31      0.37      0.26    227182
```

Fig. 4. Evaluation metrics for AdaBoost classifier



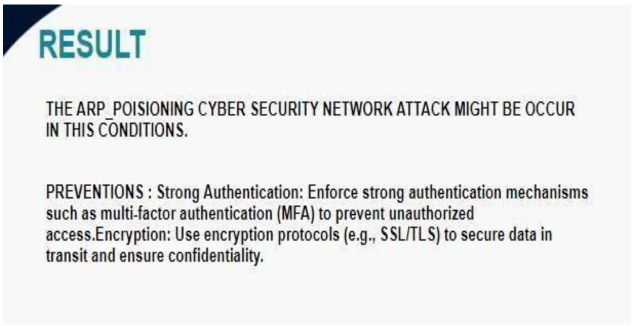
```
THE CLASSIFICATION REPORT SCORE OF RANDOM FOREST CLASSIFIER IS :

              precision    recall  f1-score   support

           0       1.00      0.99      1.00     18932
           1       1.00      1.00      1.00     18932
           2       1.00      1.00      1.00     18932
           3       1.00      1.00      1.00     18932
           4       0.98      1.00      0.99     18932
           5       1.00      1.00      1.00     18932
           6       1.00      1.00      1.00     18932
           7       1.00      1.00      1.00     18932
           8       1.00      1.00      1.00     18931
           9       1.00      1.00      1.00     18932
          10       1.00      0.99      1.00     18932
          11       1.00      1.00      1.00     18931

    accuracy                           1.00    227182
   macro avg       1.00      1.00      1.00    227182
weighted avg       1.00      1.00      1.00    227182
```

Fig. 5. Evaluation metrics for Random Forest classifier



RESULT

THE ARP_POISIONING CYBER SECURITY NETWORK ATTACK MIGHT BE OCCUR IN THIS CONDITIONS.

PREVENTIONS : Strong Authentication: Enforce strong authentication mechanisms such as multi-factor authentication (MFA) to prevent unauthorized access.Encryption: Use encryption protocols (e.g., SSL/TLS) to secure data in transit and ensure confidentiality.

Fig.6. Classification of Cyber-Attack

V. Conclusion and Future Work

In conclusion, the application of machine learning to cyberattack detection represents a major advancement in online security since it makes it possible to effectively identify and mitigate a variety of threats. Even with persistent obstacles like interpretability and data scarcity, continuous innovation is essential to improving machine learning techniques over time. The Random Forest Classifier was the most successful model among those that were looked at; it showed great precision, recall, and F1-score metrics along with an astounding accuracy of 99.82%. In order to protect digital environments for all users and sustain proactive defense against evolving cyber threats, machine learning techniques must continue to progress.

REFERENCES

1. Wongvorachan, T., He, S., & Bulut, O. (2023). A comparison of under sampling, oversampling, and SMOTE methods for dealing with imbalanced classification in educational data mining. Information, 14(1), 54. DOI: 10.3390/info14010054.
2. Viegas, E., Santin, A. O., & Abreu Jr, V. (2021). Machine Learning Intrusion Detection in Big Data Era: A Multi-Objective Approach for Longer Model Lifespans. IEEE Transactions on Network Science and Engineering, 8(1), 366-376. DOI: 10.1109/TNSE.2020.3038618
3. M. Gohil and S. Kumar, "Evaluation of Classification algorithms for Distributed Denial of Service Attack Detection," 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Laguna Hills, CA, USA, 2020, pp. 138-141, DOI: 10.1109/AIKE48582.2020.00028.
4. X. Gao, C. Shan, C. Hu, Z. Niu and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," in IEEE Access, vol. 7, pp. 82512-82521, 2019, DOI: 10.1109/ACCESS.2019.2923640.
5. Wu, P., Guo, H., & Buckland, R. (2019). A transfer learning approach for network intrusion detection. In 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA) (pp. 117-123). IEEE. DOI: 10.1109/ICBDA.2019.8713213
6. Belouch, M., El Hadaj, S., & Idhammad, M. (2018). Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Computer Science, 127, 70-78. DOI: 10.1016/j.procs.2018.01.091
7. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954-21961. DOI: 10.1109/ACCESS.2017.2762418
8. Ma T, Wang F, Cheng J, Yu Y, Chen X. A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks. Sensors. 2016; 16(10):1701. DOI: 10.3390/s16101701
9. Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. IEEE Transactions on Computers, 65(10), 2986-2998. DOI: 10.1109/TC.2016.2519914
10. Farnaaz, N., & Jabbar, M. A. (2016). Random Forest Modeling for Network Intrusion Detection System. Procedia Computer Science, 89, 213-217. DOI: 10.1016/j.procs.2016.06.047
11. Bendovschi, A. (2015, April 13-14). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Paper presented at the 7th International Conference on Financial Criminology 2015, Wadham College, Oxford, United Kingdom. DOI: 10.1016/S2212-5671(15)01077-1
12. KumarShrivas, A., & Dewangan, A. (2014). An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set. International Journal of Computer Applications, 99(15), 8-13. DOI: 10.5120/17447-5392

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details