IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

Machine Learning Technology Based Detection of Cyber Attacks & Network Attacks

Bhagyashri Dhumal[1], Dr. Monika D.Rokade[2]

PG Student, Sharad Chandra Pawar College of Engineering, Otur, Savitribai Phule University, Pune, India[1]

Asst. Professor, Department of Computer Engineering, Sharad Chandra Pawar College of Engineering, Otur, Savitribai Phule University, Pune, India[2]

ABSTRACT: The use of any sort of cloud computing platform vulnerability by cybercriminals is escalating on a global scale. The primary objectives of ethical hackers are to find problems &suggest solutions. The creation of efficient methods is urgently required in the field of cyber security. The bulk of intrusion detection methods used today are unable to attempt to deal with the intricate and dynamic nature of computer network cyber-attacks. Due to its efficiency in addressing cyber security challenges, machine learning for cybersecurity has lately become a hot topic. Critical concerns including intrusion detection, malware categorization and detection, spam detection, &phishing detection have been addressed in cyber security using machine learning techniques. ML can successfully differentiate security hazards across all technology techniques, reducing security analysts of their load even though it cannot fully automate a cyber-security system. Effective adaptive techniques, such machine learning, can therefore result in decreased false alarm rates, better detection rates, and computing and transmission cost savings. Our main goal is to address the problem that the requirements for detecting cyberattacks are fundamentally different from those for similar applications, making it far more challenging for the machine learning community working in intrusion detection to do so. The advised course of action In order to alert the system to the attack's existence in its early phases, the study's objective is to use the structure of deep neural networks for both the packet sniffer and the detection phase. The employment of reliable control algorithms in the network to separate the misbehaving agent in the leader-follower mechanism has been researched. The described control technique applies a deep neural network control system after the attack detection phase and uses the reputation algorithm to isolate the misbehaving agent. According to the results of an experiment, deep learning algorithms may identify threats more accurately than conventional techniques, making cyber security easier to implement, more proactive, less expensive, and more expensive.

KEYWORDS: Network Protocols, Wireless Network, Cyber-crime, cyber-security system, attacks, Intrusion Detection Attack (IDS), SQL Injection etc.

I.INTRODUCTION

Internet security is one of the challenging issues nowadays, considering the advances in techniques and the number of devices. A lot of data is generated so a lot of attacks to misuse that data can be expected. All these attacks and be made to the network. So, the protection of on-network from intrusion is necessary [2, 3]. The development in the field of security is not in the proportion of development that took place in the technologies, so there is a deficiency of a security model to ensure Internet security. The best way to address this challenge is to gain knowledge from the intrusions of the past. Though analysis of earlier attacks includes various levels of intrusions, the flow of data during the intrusion, environment, and network components [5].
The improvement in the intrusion detection and prevention model is necessary for the accuracy and the cost incurred. Machine learning and deep learning can deliver essential information about the attacks and the mechanism to prevent these attacks [1].

The term "cyber physical system" refers to the Information and communication technology (ICT) erawhere physical items are now linked to one another through cyber networks. The stateful firewall, sometimes referred to as attack detection and prevention, locates and prevents assaults in network traffic. A data gathering probe or an assault intended to compromise, disable, or harm a network or network resource are examples of exploits. In some cases, it might be difficult to distinguish between the two exploit goals. A flood of TCP SYN segments, for instance, can be used in a SYN flood attack to overwhelm a network and prevent it from functioning correctly, or it might be used in an IP address sweep to solicit answers from active hosts [4]. Additionally, as an attacker often conducts reconnaissance on the target prior to an attack, we might see information-gathering activities as a prelude to an upcoming attack, or more

specifically, as the first stage of an attack. As a result, it might be difficult to distinguish between reconnaissance and attack actions when using the phrase "exploit."

Our businesses and daily lives now heavily rely on the Internet and computer networks. The prevalence of harmful actions has increased as a result of our growing reliance on computers and communication networks. In the communication contexts of today, network assaults are a serious issue. In order to secure the networks' dependable operation and the security of users' information, network traffic must be tracked and analysed for harmful behaviour and assaults. In recent times, network attack detection has benefited from the use of machine learning techniques. Similarities and patterns in the network traffic may be extracted using machine learning algorithms. In contrast to signature-based techniques, extracting attack patterns does not need manual analysis. Automatically creating prediction models for network anomaly detection through the use of machine learning methods [6].

Fifth-generation networks and the advancement of artificial intelligence technologies, notably in the field of cyber security, have given rise to new dangers and challenges for wireless communication systems. We offer an overview of attack detection strategies that make use of this system's deep learning capabilities. To be more precise, we first list the core issues with network security and threat detection before introducing many cutting-edge related deep learning applications. We concentrate on attack detection systems based on categorization using deep learning techniques and built on a variety of architectures, including auto-encoders, generative adversarial networks, recurrent neural networks, and convolutional neural networks. The performance of various representation approaches is then compared, and we provide a few benchmark datasets with descriptions to show the current status of attack detection techniques employing deep learning structures. Finally, we review this research and talk about various strategies to enhance attack detection performance while considering the use of deep learning frameworks.

II.LITERATURE SURVEY

- A Review of Intrusion Detection Systems: This paper provides a comprehensive overview of intrusion detection systems, including their types, techniques, and challenges. The authors conclude that an effective IDS should be able to detect both known and unknown attacks [6].
- A Review of Intrusion Detection System Technologies: This paper surveys various intrusion detection system technologies, including signature-based, anomaly-based, and hybrid approaches. The authors highlight the importance of using multiple techniques to enhance IDS accuracy and effectiveness [7].
- A Survey of Intrusion Detection Systems: This paper presents a survey of various intrusion detection systems, including their strengths and weaknesses. The authors conclude that a hybrid IDS approach can provide better accuracy and lower false positive rates [8].
- Intrusion Detection Systems: A Comprehensive Review: This paper provides a comprehensive review of various intrusion detection systems, including their design, implementation, and evaluation. The authors conclude that an effective IDS should be able to adapt to changing attack patterns [9].
- Signature-Based Intrusion Detection Systems: A Comprehensive Survey: This paper surveys various signature-based intrusion detection systems, including their advantages and limitations. The authors conclude that signature-based IDSs are effective in detecting known attacks but are less effective against unknown attacks [10].
- Anomaly-Based Intrusion Detection Systems: A Comprehensive Survey: This paper surveys various anomaly-based intrusion detection systems, including their strengths and limitations. The authors conclude that anomaly-based IDSs are effective in detecting unknown attacks but suffer from high false positive rates [11].
- A Hybrid Approach for Intrusion Detection: This paper proposes a hybrid IDS approach that combines both signature-based and anomaly-based techniques. The authors show that the hybrid approach can provide better accuracy and lower false positive rates [12].
- Intrusion Detection Using Data Mining Techniques: This paper proposes an intrusion detection system based on data mining techniques. The authors show that their approach can provide better accuracy than traditional signature-based IDS's [13].
- Intrusion Detection Using Deep Learning Techniques: This paper proposes an intrusion detection system based on machine learning techniques. The authors show that their approach can provide better accuracy than traditional signature-based IDS's [14].
- Deep Learning for Intrusion Detection: This paper proposes an intrusion detection system based on deep learning techniques. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [15].

- Neural Networks for Intrusion Detection: This paper proposes an intrusion detection system based on neural networks. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [16].
- Support Vector Machines for Intrusion Detection: This paper proposes an intrusion detection system based on support vector machines. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [17].
- Random Forests for Intrusion Detection: This paper proposes an intrusion detection system based on random forests. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [18].
- Bayesian Networks for Intrusion Detection: This paper proposes an intrusion detection system based on Bayesian networks. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [19].
- Fuzzy Logic for Intrusion Detection: This paper proposes an intrusion detection system based on fuzzy logic. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting unknown attacks [20].
- Genetic Algorithms for Intrusion Detection: This paper proposes an intrusion detection system based on genetic algorithms. The authors show that their approach can provide better accuracy than traditional signature-based IDSs and is effective in detecting [21].

III.PROBLEM STATEMENT

- To address the aforementioned challenges, we proposed a novel algorithm and build an web based application for detection of different four types of attacks which is, SQL Injection, Cross-Site Scripting (XSS), Phishing Attacks, and Normal Intrusion Detection Attack (IDS).
- In Proposed studies shows that the problem definition gets more specific for any attack type and includes an expanded definition of the attack and its behavior. Further, we confirmed that the performance of neural network increases with increase in accuracy and performance of algorithms.

IV.SCOPE OF THE PROJECT

The computer science branch of machine learning assemblages and fragments behaviours and entities employing data artificial intelligence and template identification techniques. On fresh data, prediction tasks may be performed using these previously identified patterns and correlations that machine learning algorithms have learned. Machine learning algorithms are employed in many different applications nowadays, which has an impact on our daily lives.
Due to the following qualities, which make it simple to use, comprehend, and change, this project has a broad reach:

- Easy to detection of cyber and network attacks.
- To save the environment by using machine learning techniques
- To increase the accuracy and efficiency of the attacks detectionprocedure.
- Management of Kaggle datasets and its feature selection.

V.PROPOSED SYSTEM

The use of any computing environment flaw by cybercriminals is causing them to proliferate throughout the world. Assessment of vulnerabilities and the provision of mitigation techniques are ethical hackers' main concerns. A critical need in the cyber security community's toolkit is the development of effective techniques. For the most part, IDS methods deployed today cannot deal with the dynamic &complicated characteristics of computer network cyberattacks. Due to ML's success in addressing cyber security challenges, the topic of machine learning has lately taken on significant relevance. Major challenges in cyber security, including intrusion detection, malware categorization and detection, spam detection, and phishing detection, have been addressed using ML techniques. Machine learning may identify cyber security risks more effectively than other software-oriented techniques, relieving pressure on security analysts even if it cannot fully automate a cyber-security system. As a result of effective adaptive methods, detection rates can be increased, false alarm rates reduced, and calculation and transmission costs reduced. Machine learning approaches are examples. Our main goal is to show that the complexity of detecting attacks is fundamentally different

from the difficulties of these other applications, making it significantly more difficult for the machine learning community to properly assist intrusion detection.

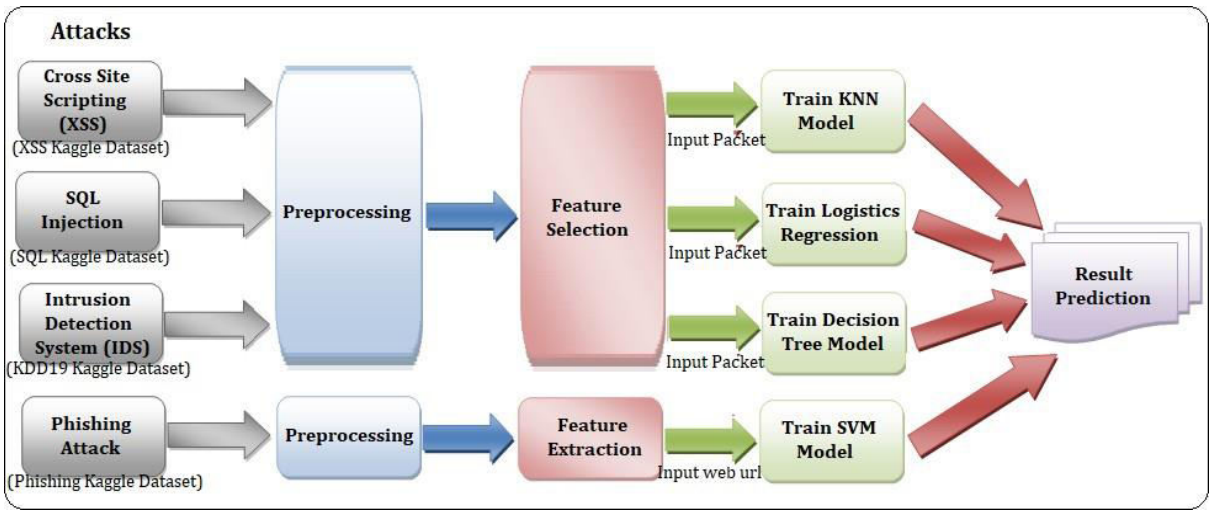

Fig.1: System Architecture

A cyberattack may be trained for and detected using machine learning techniques. An email alert may be issued to the security users as soon as the threat is discovered. An assault can be classified as a DoS/DDoS attack using any classification technique. One example of a classification algorithm and deep inspection technique is Novel Sniffer Detection Algorithm, a supervised learning method that examines data and recognises patterns. Our greatest option right now is early identification, which will help reduce the risk of irreversible harm such events can do, as we cannot foresee when, why, or how an assault will occur and absolute prevention cannot be assured. In order to reduce the effect of cyberattacks, organisations might adopt current solutions or develop their own. The ideal system would be one with little need for human involvement.

VI. PERFORMANCE ANALYSIS

Performance analysis of a system that uses machine learning algorithms to detect cyber and network attacks would involve evaluating the system's ability to accurately identify and classify different types of attacks. This analysis would typically involve the following steps:

- Data collection: Collect a dataset of both normal network traffic and known cyber-attacks. This dataset should be representative of the types of traffic and attacks that the system will encounter in a real-world scenario.
- Feature extraction: Extract relevant features from the dataset that can be used as input to the machine learning algorithms. These features could include network traffic patterns, protocol usage, and other characteristics of the traffic.
- Model training: Train the machine learning algorithms using the feature-extracted dataset. This step will typically involve using a portion of the dataset for training and reserving the rest for testing.
- Model evaluation: Evaluate the performance of the trained machine learning algorithms using various metrics, such as accuracy, precision, recall, and F1-score. These metrics will give an idea of how well the model is able to detect and classify different types of attacks.
- Model fine-tuning: Based on the evaluation results fine-tune the model by adjusting the parameters and/or the features used.
- Real-world testing: Test the model in a real-world scenario to evaluate its performance in a more realistic setting.

It is also important to note that a system like this would require continuous monitoring, updating and retraining to adapt to the changing threat landscape. Additionally, it would be ideal to test the system against various types of attacks and adversarial attacks to evaluate its robustness.

VII. CONCLUSIONS

This study attempted to apply the resilient control consensus approach in complicated discrete cyber-physical networks with a variety of local assaults disabled. It was discovered that by using this control approach, the system may continue to function normally even in the midst of cyberattacks, isolate the attacked node, and maintain its stability. It was discovered that the system performs better when a deep neural network with seven hidden layers is utilised, using the neural network used in this study as an example. Additionally, a deep layer network with a linear function performs better when combined with a recurrent neural network. In light of this, the system can be regarded to be less complicated. So Systems may analyse patterns and learn from them with the use of deep learning techniques, which can be used to stop similar assaults and react to altering behaviour. In conclusion, ML has the ability to significantly improve the effectiveness, cost, and proactiveness of cyber security. The control system takes choices based on the observations of the system's state that the neural network reports, and if there is an attack, it recognises it and isolates it so as not to negatively impact the behaviour of other agents. We looked at a number of significant algorithms for attack detection that are based on different ML approaches. Due to the properties of ML techniques, it is possible to design assaults with high detection rates and low false positive rates, while also allowing the system to quickly adapt to shifting hostile behaviour. Any firm that does not immediately embrace these strategies runs the danger of having its systems or data compromised.

REFERENCES

[1] Z. N. Zarandi and I. Sharifi, "Detection and Identification of Cyber-Attacks in Cyber-Physical Systems Based on Machine Learning Methods," 2020 11th International Conference on Information and Knowledge Technology (IKT), 2020, pp. 107-112, doi: 10.1109/IKT51791.2020.9345627.

[2] Nurjahan, F. Nizam, S. Chaki, S. Al Mamun and M. S. Kaiser, "Attack detection and prevention in the Cyber Physical System," 2016 International Conference on Computer Communication and Informatics (ICCCI), 2016, pp. 1-6, doi: 10.1109/ICCCI.2016.7480022.

[3] Ding Chen, Qiseng Yan, Chunwang Wu and Jun Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," Journal of Physics: Conference Series, Volume 1757, International Conference on Computer Big Data and Artificial Intelligence (ICCBDAI 2020) 24-25 October 2020, Changsha, China

[4] Ercan NurcanYılmaz, SerkanGönen, "Attack detection/prevention system against cyber-attack in industrial control systems," Computers & Security Volume 77, August 2018, Pages 94-105

[5] Arpitha. B, Sharan. R, Brunda. B. M, Indrakumar. D. M, Ramesh. B. E, "Cyber Attack Detection and notifying system using ML Techniques," International Journal of Engineering Science and Computing (IJESC), Volume 11, Issue No.06

[6] Yirui Wu, Dabao Wei, and Jun Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey," Security Threats to Artificial Intelligence-Driven Wireless Communication Systems, 2020.

[7] Rafał Kozik, Michał Choraś, "Machine Learning Techniques for Cyber Attacks Detection," Image Processing and Communications Challenges 5, pp 391-398, Springer International Publishing Switzerland 2014.

[8] Nutjahan, Farhana Nizam, Shudarshon Chaki, Shamim Al Mamun, M. Shamim, "Attack Detection and Prevention in the Cyber Physical System," 2016 International Conference on Computer Comrnunication and Informatics (IEEE -2016), Jan. 07 - 09, 2016, Coimbatore, India

[9] Yong Fang, Cheng Huang, Yijia Xu and Yang Li, "RLXSS: Optimizing XSS Detection Model to Defend Against Adversarial Attacks Based on Reinforcement Learning," Future Internet 2019.

[10] Pratik Rajendra Chougule, Aniket Sanjay Kumbhar, Vinayak Vasant Pachange, Karan Dinkar Phonde, S. P. Phadtare, "Phishing Websites Detection using Python," Journal of Web Development and Web Designing, Volume-5, Issue-2 (May-August, 2020)

[11] Rishikesh Mahajan, Irfan Siddavatam, "Phishing Website Detection using Machine Learning Algorithms," International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 23, October 2018

[12] Vishnu. B. A, Ms. Jevitha. K. P, "Prediction of Cross-Site Scripting Attack Using Machine Learning Algorithms," Conference Paper • October 2014.

[13] Shinelle Hutchinson, Zhaohe Zhang, and Qingzhong Liu, "Detecting Phishing Websites with Random Forest," Third International Conference, MLICOM 2018, Hangzhou, China, July 6-8, 2018, Proceedings

[14] Ines Jemal, Omar Cheikhrouhou, Habib Hamam and Adel Mahfoudhi, "SQL Injection Attack Detection and Prevention Techniques Using Machine Learning," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 6 (2020) pp. 569-580

[15] Fawaz A. Mereani, and Jacob M. Howe, "Detecting Cross-Site Scripting Attacks Using Machine Learning," Springer International Publishing AG, part of Springer Nature 2018.
[16] D. Larson, ``Distributed denial of service attacksholding back the flood," Netw. Secur., vol. 2016, no. 3, pp. 5-7, 2016.
[17] R. C. Staudemeyer, ``Applying long short-term memory recurrent neural networks to intrusion detection," South Afr. Comput. J., vol. 56, no. 1, pp. 136-154, 2015.
[18] S. Venkatraman and M. Alazab, ``Use of data visualisation for zero-day Malware detection," Secur. Commun. Netw., vol. 2018, Dec. 2018, Art. no. 1728303. [Online]. Available: https://doi.org/10.1155/2018/1728303
[19] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, ``A detailed investigation and analysis of using machine learning techniques for intrusion detection," IEEE Commun. Surveys Tuts., to be published. doi: 10.1109/comst.2018.2847722.
[20] A. Azab, M. Alazab, and M. Aiash, ``Machine learning based botnet identification trafc," in Proc. 15th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (Trustcom), Tianjin, China, Aug. 2016, pp. 1788-1794.
[21] R. Vinayakumar. (Jan. 2, 2019). Vinayakumarr/Intrusion-Detection V1 (Version V1). [Online]. Available: http://doi.org/10.5281/zenodo.2544036
[22] M. Tang, M. Alazab, Y. Luo, and M. Donlon, ``Disclosure of cyber security vulnerabilities: time series modelling," Int. J. Electron. Secur. Digit. Forensics, vol. 10, no. 3, pp. 255-275, 2018.
[23] Y. LeCun, Y. Bengio, and G. Hinton, ``Deep learning," Nature, vol. 521, no. 7553, p. 436, 2015.
[24] Y. Xin et al., ``Machine learning and deep learning methods for cyber-security," IEEE Access, vol. 6, pp. 35365-35381, 2018
[25] N. Hubballi, S. Biswas, and S. Nandi, ``Sequencegram: n-gram modelling of system calls for program based anomaly detection," in Proc. 3rd Int. Conf. Commun. Syst. Netw. (COMSNETS), Jan. 2011, pp. 1-10.
[26] N. Hubballi, ``Pairgram: Modeling frequency information of lookahead pairs for system call based anomaly detection," in Proc. 4th Int. Conf. Commun. Syst. Netw. (COMSNETS), Jan. 2012, pp. 1-10
[27] S. Huda, J. Abawajy, M. Alazab, M. Abdollalihian, R. Islam, and J. Yearwood, ``Hybrids of support vector machine wrapper and filter based framework for malware detection," Future Gener. Comput. Syst., vol. 55, pp. 376-390, Feb. 2016.
[28] M. Alazab et al., ``A hybrid wrapper-filter approach for Malware detection," J. Netw., vol. 9, no. 11, pp. 2878-2891, 2014.
[29] L. Ertöz, M. Steinbach, and V. Kumar, ``Finding clusters of different sizes, shapes, and densities in noisy, high dimensional data," in Proc. SIAM Int. Conf. Data Mining, 2013, pp. 47-58
[30] C. Kolias, G. Kambourakis, and M. Maragoudakis, ``Swarm intelligence in intrusion detection: A survey," Comput. Secur., vol. 30, no. 8, pp. 625-642, 2011. doi: 10.1016/j.cose.2011.08.009.
[31] C. yin, Y. Zhu, J. Fei, and X. He, ``A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954-21961, 2017.
[32] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, ``A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS), 2016, pp. 21-26.
[33] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, ``Long short term memory recurrent neural network classifier for intrusion detection," in Proc. Int. Conf. Platform Technol. Service (PlatCon), Feb. 2016, pp. 1-5.
[34] F. A. B. H. Ali and Y. Y. Len, ``Development of host based intrusion detection system for log les," in Proc. IEEE Symp. Bus., Eng. Ind. Appl. (ISBEIA), Sep. 2011, pp. 281-285.
[35] E. Aghaei and G. Serpen, ``Ensemble classifier for misuse detection using N-gram feature vectors through operating system call traces," Int. J. Hybrid Intell. Syst., vol. 14, no. 3, pp. 141-154, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

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