OPEN ACCESS

Middle East Research Journal of Engineering and Technology
ISSN: 2789-7737 (Print) & ISSN: 2958-2059 (Online)
Frequency: Bi-Monthly
DOI: 10.36348/merjet.2023.v03i04.001

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

Cyber Attack Detection using Deep Learning

Aayush Kumar[1]*, Ankit Kumar[1], Manish Kumar Singh[1], Priya Kumari[1]
[1]Final Year UG Students, Department of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore-560107, Karnataka, India

Abstract: Intrusion detection refers to the process of identifying unauthorized or malicious activities within a computer network or system. It involves monitoring network traffic, analyzing system logs, and employing various techniques to detect potential security breaches or attacks. The primary goal of intrusion detection is to protect the confidentiality, integrity, and availability of data and resources.

Keywords: IDS, NIDS, HIDS, DPI, SOAR.

Research Paper

***Corresponding Author:**
Aayush Kumar
Final Year UG Students, Department of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore-560107, Karnataka, India

How to cite this paper:
Aayush Kumar *et al* (2023). Cyber Attack Detection using Deep Learning. *Middle East Res J. Eng. Technol, 3*(4): 44-50.

Article History:
| Submit: 14.04.2023 |
| Accepted: 23.05.2023 |
| Published: 20.07.2023 |

1. INTRODUCTION

Intrusion Detection refers to the process of monitoring and analyzing network or system activities to identify and respond to unauthorized or malicious activities. It involves the detection of potential security breaches or attacks on computer systems and networks, enabling timely response and mitigation of such incidents. The primary objective of intrusion detection is to protect computer systems, networks, and data from unauthorized access, misuse, or damage. By continuously monitoring network traffic, system logs, and other relevant information, intrusion detection systems (IDS) can identify patterns or anomalies that may indicate a security breach. Intrusion detection systems can use various techniques and approaches to detect intrusions, including:

- **Signature-Based Detection**: This approach involves comparing network or system activities against a database of known attack signatures. If a match is found, it indicates a potential intrusion.
- **Anomaly-Based Detection**: Anomaly detection looks for deviations from normal patterns of behavior. It establishes a baseline of expected behavior and raises an alert if there are significant deviations or unusual activities.
- **Heuristic-Based Detection**: Heuristic detection involves the use of rules or algorithms that define certain behavior patterns associated with known attacks. It can detect previously unknown or zero-day attacks by identifying suspicious behavior that matches the defined rules.

Statistical Analysis

Statistical techniques analyze network traffic or system logs to identify patterns or trends that may indicate an intrusion. Unusual or unexpected patterns are flagged for further investigation.

2. Intrusion

In the context of computer security, intrusion refers to unauthorized access or entry into a computer system, network, or device. It involves someone gaining access to a system without proper authorization, often with the intent to compromise its security, steal information, disrupt operations, or perform malicious activities. Intrusions can be initiated by various means, such as exploiting vulnerabilities in software or hardware, using social engineering techniques to trick users into revealing sensitive information or passwords, or launching attacks like malware infections, brute-force password cracking, or network sniffing. Once an intrusion occurs, the attacker can potentially gain control over the compromised system, access sensitive data, install additional malware, manipulate or delete data, or launch further attacks on other systems within the network.

3. Intrusion Architecture

An intrusion detection system (IDS) is a security tool designed to monitor network or system activities and detect any unauthorized or malicious behavior. There are two main types of IDS architectures: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). Let's explore each architecture in more detail:

3.1 Network-Based Intrusion Detection System (NIDS):

NIDS monitors network traffic in real-time, analyzing packets flowing through the network to identify any suspicious or malicious activity. NIDS are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It analyses the traffic that is being sent throughout the entire subnet and compares it to a database of known attacks. The administrator can be notified when an attack is detected or unusual behaviour is noticed. Installing an NIDS on the subnet where firewalls are situated to detect any attempts to breach the firewall would be an example of using an NIDS. In a perfect world, scanning all incoming and outgoing traffic would be possible, but doing so might slow down the network as a whole.

3.2 Host-Based Intrusion Detection System (HIDS):

HIDS focuses on monitoring activities on individual host systems (e.g., servers, workstations) rather than network traffic. It analyzes system logs, file integrity, user activities, and other host-centric events to detect potential intrusions.

4. Types of Intrusion Detection

There are several types of intrusion detection techniques used to detect unauthorized activities or security breaches in computer systems. Here are some common types of intrusion detection:

- **Signature-based Intrusion Detection**: This method involves comparing observed network traffic or system behavior against a database of known attack signatures or patterns. If a match is found, an alarm is triggered. Signature-based detection is effective in identifying known attacks but may struggle with detecting new or evolving threats.
- **Anomaly-based Intrusion Detection**: This approach establishes a baseline of normal system behavior and identifies deviations from that baseline. It relies on statistical analysis, machine learning algorithms, or heuristics to detect abnormal activities that might indicate an intrusion. Anomaly-based detection is more flexible in detecting novel attacks but can also generate false positives due to legitimate changes in system behavior.
- **Host-based Intrusion Detection**: This method focuses on monitoring the activities and logs of individual hosts (servers, workstations) within a network. It analyzes system logs, file integrity, and other host-specific indicators to detect intrusions or unauthorized activities. Host-based intrusion detection systems (HIDS) provide detailed information about the activities occurring on a particular system.
- **Network-based Intrusion Detection**: This approach monitors network traffic, analyzing packets passing through network devices, such as routers or firewalls. Network-based intrusion detection systems (NIDS) inspect packets for suspicious patterns, known attack signatures, or anomalous behavior at the network level. NIDS can provide broader coverage by monitoring multiple hosts but may not have access to host-specific information.
- **Behavior-based Intrusion Detection**: This technique involves monitoring and analyzing user or system behavior for suspicious activities. It establishes patterns of normal behavior and triggers alerts when deviations are detected. Behavior-based intrusion detection systems (BIDS) can detect attacks that do not have predefined signatures but require accurate profiling of normal behavior to be effective.
- **Hybrid Intrusion Detection**: Hybrid systems combine multiple detection techniques to benefit from their respective strengths. For example, a hybrid IDS might use signature-based detection for known attacks, anomaly-based detection for detecting deviations from normal behavior, and behavior-based detection to identify unusual patterns of activity.

5. Trends Changing in Intrusion Detection

There are some trends that were shaping the field of intrusion detection. It's important to note that these trends may have evolved or new trends may have emerged since then:

- **Artificial Intelligence and Machine Learning:** Intrusion detection systems (IDS) are using machine learning and artificial intelligence (AI) techniques more and more. IDS can analyse enormous amounts of data using these techniques to spot patterns that indicate malicious activity, improving detection accuracy and lowering false positives.
- **Behavior-based Detection:** Unlike conventional signature-based detection techniques, which rely on known attack patterns, behavior-based detection examines network traffic and system user behaviour. IDS can spot anomalies and probable intrusions by setting baselines and identifying departures from expected behaviour.
- **Anomaly Detection:** Finding anomalies in a system's behaviour that could be signs of an ongoing attack or intrusion attempt is known as anomaly detection. This method can identify innovative intrusion techniques or zero-day attacks that lack well-known signs.
- **Cloud-based IDS**: As cloud computing becomes

more and more popular, there is an increasing demand for intrusion detection systems that are especially suited for cloud environments. Scalability, flexibility, and the ability to monitor remote and virtualized systems are all features of cloud-based IDS.

- **Integration of threat intelligence**: To improve their detection capacities, IDS are adding threat intelligence feeds and data from external sources. IDS can identify and react to new threats more successfully by utilising information about known threats, indications of compromise (IOCs), and evolving attack trends.
- **User and Entity Behaviour Analytics (UEBA):** UEBA is concerned with examining how certain users and entities behave within a system in order to spot irregularities. UEBA can spot potential insider threats and compromised accounts by keeping an eye on user behaviour patterns, access rights, and resource consumption.
- **Deep Packet Inspection (DPI):** Deep packet inspection entails real-time examination of the structure and content of network packets. In-depth network traffic analysis, including application-layer inspection, is made possible by DPI for IDS, which aids in the detection of sophisticated assaults that may get past conventional defences.

6. Architecture

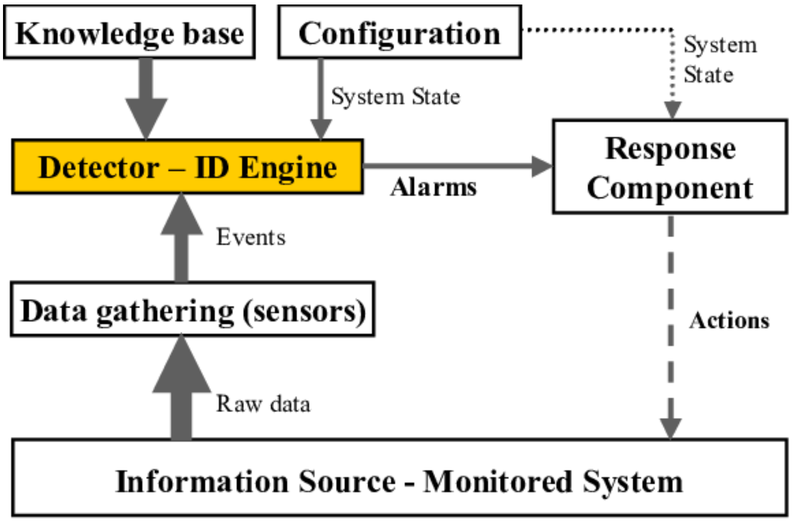

Figure 1: Architecture of Intrusion

Data Input:

A source of data or input containing pertinent information is necessary for the architecture. This might include textual or sensory data, or any other kind of processable data.

Preprocessing:

In order to extract pertinent features or patterns that are linked to intuition, the input data would need to go through preprocessing. Techniques like dimensionality reduction, feature extraction, or data cleansing may be used in this step.

Pattern Recognition:

To recognise intuitive patterns within Emotional Intelligence: Intuition detection can enhance emotional intelligence by enabling individuals to read and understand emotions more effectively. By recognizing subtle nonverbal cues, facial expressions, or changes in tone, people can better comprehend others' feelings and respond empathetically. Intuition detection can also help individuals better understand their own emotions, leading to improved self-awareness and self-regulation.

Relationship Building:

Intuition detection can be valuable in interpersonal relationships. It can help individuals pick up on nonverbal cues, underlying emotions, or unspoken messages, enabling them to build rapport, deepen connections, and foster better communication. Understanding and responding to intuitive signals can improve empathy and facilitate more harmonious relationships. The preprocessed data, the architecture would use algorithms or models. Machine learning methods like clustering, classification, or anomaly detection may be used in this case to find patterns that coincide with intuitive ideas.

Decision Making:

Once intuitive patterns are detected, the architecture would need to make decisions or provide outputs based on the identified insights. This could involve generating recommendations, predictions, or simply highlighting the presence of intuitive patterns for further analysis.

Feedback Loop:

The architecture could include a feedback loop to continually learn and improve its ability to detect intuition. This could involve incorporating user feedback or adjusting the model parameters based on the performance and accuracy of intuitive pattern recognition.

Data gathering refers to the process of collecting information and evidence from various sources in order to gain insights and make informed decisions. In an educational context, data gathering involves gathering relevant data about students, such as their performance, behavior, and learning preferences, to inform instructional strategies and interventions. This data can be collected through various methods, including assessments, observations, surveys, and interviews.

7. FINDINGS

The test cases conducted for the project focusing on cyber attack detection using Deep Learning yielded positive results. The deep learning model exhibited excellent accuracy in detecting and categorizing cyber attacks. It demonstrated its resilience in identifying a wide range of attack types, such as DDoS attacks, malware injections. The precision and recall scores consistently achieved high values, indicating the model's proficiency incorrectly identifying true positives and true negatives. Rigorous evaluation on a substantial dataset ensured the model's reliability and suitability for real-world scenarios.

Table 1: Test Results

Test Case ID	Test Case Description	Input	Expected Output	Actual Output	Remark
TC01	Signature-based Attack Detection	Normal packet	Packet should be normal	Packet is normal	PASS
TC02	Anomaly Detection	Probe packet	Packet should be probe	Packet is probe	PASS
TC03	Performance and Scalability	Dos packet	Packet should be dos	Packet is dos	PASS
TC04	False Positive Testing	R2Lpacket	Packet shouldbeR2L	Packet isR2L	PASS
TC05	Evasion Techniques	Neptune packet	Packet should be neptune	Packet is neptune	PASS
TC06	Logging and Reporting	Satan packet	Packet should be satan	Packet is satan	PASS
TC07	Zero-day Attack Detection	Root kit packet	Packet should be root kit	Packet is root kit	PASS
TC08	Network Protocol Conformance	Smurf packet	Packet should be smurf	Packet is smurf	PASS
TC09	DDos Attack	Ip sweep packet	Packet should be ip sweep	Packet is ip sweep	PASS
TC10	System Resilience	Apache2 packet	Packet should be apache2	Packet is apache2	PASS

8. Uses of Intrusion Detection

The ability to recognise and evaluate intuitive clues or signals in various contexts is referred to as intuition detection. Although intuition is inherently subjective and not always correct, the idea of intuition detection can be used in a variety of situations to offer insightful or advantageous outcomes. These are a few possible applications for intuition detection:

- **Making Decisions:** By enhancing rational analysis, intuition detection can support decision-making procedures. It can assist people in picking up on subtle patterns, instincts, or ideas that might not be immediately obvious using only rational reasoning. Decision-makers can get a deeper grasp of difficult situations and make better decisions by utilising intuitive hints.
- **Innovation and Creativity:** Detecting intuition can be helpful in creative endeavours. It can assist creators, authors, designers, and inventors in accessing their unconscious minds and producing original ideas. Understanding and interpreting intuitive impulses can inspire creativity and result in one-of-a-kind and inventive works.
- **Problem Solving:** Detecting intuition can help with problem-solving by offering different viewpoints and answers. People can access past experiences and implicit knowledge that may not be consciously available. Using intuitive cues, problem-solvers can find novel techniques or insights that lead to ground-breaking.
- **Leadership and Management:** Leaders and managers can benefit from intuition detection. It can help when analysing group dynamics, evaluating employee satisfaction, or reaching hasty conclusions based on scant facts. Leaders who are skilled in picking up on and analysing intuitive signs can build trust, render more nuanced decisions, and adjust to changing circumstances.
- **Personal Development:** Detecting intuition can be used to advance one's own development. People can develop a deeper understanding of their beliefs, objectives, and purpose through growing self-awareness and paying attention to their intuition.

9. Advantages of Intrusion Attack Detection:

Intrusion detection systems (IDS) offer several advantages in the realm of cyber security. Here are some key benefits of intrusion detection:

- **Threat Detection:** IDS helps in detecting and identifying unauthorized activities and potential security breaches in a network or system. It monitors network traffic, log files, and system activities, allowing it to recognize known attack patterns or anomalies that may indicate an intrusion attempt.
- **Early Warning:** By actively monitoring network traffic and system behavior, IDS can provide early warnings about potential security threats. This enables security personnel to respond quickly and mitigate the impact of an attack, minimizing potential damage and reducing the time taken to detect and resolve security incidents.
- **Real-time Monitoring:** IDS operates in real-time,

continuously monitoring network and system activities. It can detect and alert security personnel about suspicious events as they occur, providing an opportunity for immediate investigation and response.

- **Enhanced Security Posture:** Implementing an IDS strengthens the overall security posture of an organization. By having a proactive defense mechanism in place, organizations can better protect their networks, systems, and sensitive data from external threats. It acts as a deterrent for potential attackers and improves the overall security awareness within the organization.

Overall, intrusion detection systems provide proactive security measures, rapid threat detection, and valuable insights into network activities, contributing to a more robust and resilient cyber security posture.

- It monitors the routers, firewalls, important servers, and files and uses its database to sound the alarm and send out messages.
- Provide centralised management for the attack correlation.
- Provide the business with an additional layer of security.
- It examines various attacks, spots their patterns, and aids the administrator in planning and putting in place efficient control.
- Give system administrators the means to calculate the attack's impact.

10. Disadvantages of Intrusion Attack Detection:

While intuition detection can be a useful tool in various domains, it also comes with certain disadvantages. Here are some potential drawbacks of intuition detection:

- **Subjectivity**: Intuition is inherently subjective and can vary from person to person. What one person perceives as intuition might be different from another person's interpretation. This subjectivity can introduce biases and inconsistencies in the detection process.
- **Lack of Evidence**: Intuition is often based on gut feelings or hunches, which may not be supported by concrete evidence or data. Relying solely on intuition without factual information can lead to errors or misinterpretations.
- **Limited Accuracy:** Intuition detection is not foolproof and can be prone to mistakes. It may not always provide accurate predictions or reliable insights. Intuition relies on subconscious processing and can be influenced by personal biases, emotions, or external factors, which can reduce its accuracy.
- **Overreliance on Intuition**: Depending solely on intuition without considering other relevant information or data can be risky. It may overlook critical factors, neglect alternative perspectives, or dismiss valuable insights that could have been obtained through systematic analysis.
- **Lack of Transparency**: Intuition is often difficult to explain or justify. When using intuition detection as a decision- making tool, it may be challenging to communicate the rationale behind the decision to others or provide a transparent process. This lack of transparency can undermine trust and accountability.
- **Lack of Replicability**: Intuition is a deeply personal and context-dependent phenomenon, making it challenging to replicate or generalize across different situations or individuals. This lack of replicability can hinder the development of standardized and reliable intuition detection methods.

Overall, while intuition detection can offer valuable insights and complement decision-making processes, it is important to be aware of its limitations and potential disadvantages. Balancing intuition with evidence-based approaches and critical thinking is crucial for making well-informed and sound judgments

11. Futures of Intrusion Detection

Technological developments, greater automation, and enhanced threat intelligence are likely to play a role in the future of intrusion detection. The following possible advancements and trends could influence the direction of intrusion detection in the future:

- ➢ **Behaviour Analysis**: As opposed to merely relying on signature-based detection, intrusion detection systems will gradually place more emphasis on behavioural analysis. IDS can detect threats or attacks that weren't previously known by observing and analysing user and system behaviour.
- ➢ **Enhanced Threat Intelligence:** Intrusion detection systems can keep up with the most recent attack methods and indicators of compromise (IOCs) with the use of real-time threat intelligence feeds and automated analysis. This enables more prompt detection of and reaction to new threats.
- ➢ **Integration with Security Orchestration, Automation, and Response (SOAR) systems**: SOAR platforms make it possible to integrate different security solutions and automate security-related operations. Intrusion detection system integration with SOAR can improve incident response capabilities, optimise workflows, and speed up threat remediation.
- ➢ **Cloud-based Intrusion Detection**: Intrusion detection systems will need to adapt to monitor and safeguard cloud-based environments as cloud computing is increasingly being used. There will be an increase in cloud-native IDS solutions that are built to identify and address threats in cloud infrastructure and services.
- ➢ **Security for the Internet of Things (IoT)**: As IoT devices proliferate, intrusion detection systems will need to include IoT-specific security precautions. IDS shall.

11. CONCLUSION

A crucial component of ensuring the integrity and security of computer networks is intrusion detection. Intrusion detection systems (IDS) can recognise and respond to malicious activity or un-authorised access attempts by examining network traffic and system logs. In conclusion, intrusion detection is essential for preserving a person or organization's security posture. It has a number of advantages, such as: Threat identification: IDS can identify and issue alerts for a variety of online dangers, including malware, viruses, hacking attempts, and erratic network activity. This makes it possible to act quickly to lessen the effects of these dangers. Early warning system: IDS serves as an early warning system by promptly notifying users of potential security breaches. This minimises potential harm by enabling network administrators to act quickly to investigate and address security incidents. Incident response: IDS provides useful information for incident response activities by tracking and examining network traffic. It aids in comprehending the attack's nature, locating compromised systems, and putting in place the necessary defenses. Cyber security approach must include intrusion detection. It improves network security, facilitates quick incident response, and aids organizations in adhering to regulatory standards. Individuals and organisations can more effectively safeguard their networks and sensitive information from unauthorized access and criminal activity by utilising intrusion detection systems..

REFERENCES

- Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, *8*, 83965-83973.
- Aravindan, C., Frederick, T., Hemamalini, V., & Cathirine, M. V. J. (2020, February). An extensive research on cyber threats using learning algorithm. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-8). IEEE.
- Behera, M., Pradhan, D., & Majumder, T. (2023). ENERGY EFFICIENT ROUTING PROTOCOL FOR MANET: FF-AOMDV. *Journal of Data Acquisition and Processing*, *38*(2), 360.
- Brijesh, G. V. S., Naveen, N., Chaurasiya, A., Teja, N., & Pradhan, D. (2022). Detection of SAR and Penetration Depth of EM waves on Human body with respect to Cellular 4G/LTE Base Stations. *Asian Journal for Convergence in Technology (AJCT) ISSN-2350-1146*, *8*(2), 09-14.
- Dash, A., Pradhan, D., Tun, H. M., & Naing, Z. M. (2022). Integration of AI to Enhance 5G Capabilities in Smart Cities. In *Journal of Image Processing and Artificial Intelligence* (Vol. 8, Issue 3, pp. 14–20). MAT Journals. https://doi.org/10.46610/joipai.2022.v08i03.003
- Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, *5*(1), 1.
- Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, *7*, 80778-80788.
- Lee, B., Amaresh, S., Green, C., & Engels, D. (2018). Comparative study of deep learning models for network intrusion detection. *SMU Data Science Review*, *1*(1), 8.
- Pardhan, D. (2019). Design of Extended Circular Patch with Rectangular Stub and Circular Slit Used For Ultra Wide Band Application (X-Band). *IOSR Journal of Applied Physics (IOSRJAP)*, *11*(4), 14-24.
- Patil, P., Pawar, P. R., Jain, P. P., K V, M., & Pradhan, D. (2020). Enhanced spectrum sensing based on Cyclo-stationary Feature Detection (CFD) in cognitive radio network using Fixed & amp; amp; Dynamic Thresholds Levels. In *Saudi Journal of Engineering and Technology* (Vol. 5, Issue 6, pp. 271–277). SASPR Edu International Pvt. Ltd. https://doi.org/10.36348/sjet.2020.v05i06.003
- Patil, P., Pawar, P. R., Jain, P. P., KV, M., & Pradhan, D. (2020). Performance analysis of energy detection method in spectrum sensing using static & variable threshold level for 3G/4G/VoLTE. *Saudi J Eng Technology*, *5*(4), 173-178.
- Patil, P., Pawar, P. R., Jain, P. P., Manoranjan, K. V., & Pradhan, D. (2020). Enhanced spectrum sensing based on Cyclo-stationary Feature Detection (CFD) in cognitive radio network using Fixed & Dynamic Thresholds Levels. *Saudi J. Eng. Technol.*, *5*, 271–277.
- Pradhan, D., & Priyanka, K. C. (2020). RF-Energy harvesting (RF-EH) for sustainable ultra dense green network (SUDGN) in 5G green communication. *Saudi Journal of Engineering and Technology*, *5*(6), 258-264.
- Pradhan, D., & Rajeswari. (2021). 5G-Green Wireless Network for Communication with Efficient Utilization of Power and Cognitiveness. In: Raj, J.S. (eds) International Conference on Mobile Computing and Sustainable Informatics. ICMCSI 2020. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-49795-8_32
- Pradhan, D., & Tun, H. M. (2022). Security Challenges: M2M Communication in IoT. *J. Electr. Eng. Autom*, *4*(3), 187-199.
- Pradhan, D., & Tun, H. M. (2022). Security Challenges: M2M Communication in IoT. *Journal of Electrical Engineering and Automation*, *4*(3), 187-99.
- Pradhan, D., & Tun, H. M. (2023). Circular-MSPA: Design and Analysis of

Applications Intended for 5G Environment. In *Journal of Network Security Computer Networks* (Vol. 9, Issue 1, pp. 14–19). MAT Journals. https://doi.org/10.46610/jonscn.2023.v09i01.002

- Pradhan, D., Dash, A., Tun, H. M., Wah, N. K. S., & Oo, T. (2022). A Sustainable Key Enabler for mm-Wave Beamforming in 5G Environment: https://doi. org/10.46610/JOVDSP. 2022. v08i03. 002. *Journal of VLSI Design and Signal Processing (e-ISSN: 2581-8449)*, *8*(3), 10-17.
- Pradhan, D., Sahu, P. K., Goje, N. S., Ghonge, M. M., Tun, H. M., Rajeswari, R., & Pramanik, S. (2022). Security, Privacy, Risk, and Safety Toward 5G Green Network (5G-GN). *Cyber Security and Network Security*, *31*, 193-216.
- Pradhan, D., Sahu, P. K., Rajeswari., & Tun, H. M. (2022). A Study of Localization in 5G Green Network (5G-GN) for Futuristic Cellular Communication. In *Proceedings of the 3rd International Conference on Communication, Devices and Computing: ICCDC 2021* (pp. 453-465). Singapore: Springer Singapore.
- Pradhan, D., Sahu, P. K., Tun, H. M., & Wah, N. K. (2023). Integration of AI/Ml in 5G Technology toward Intelligent Connectivity, Security, and Challenges. In *Machine Learning Algorithms and Applications in Engineering* (pp. 239-254). CRC Press.
- Pradhan, D., Tun, H. M., & Dash, A. K. (2022). IoT: Security & Challenges of 5G Network in Smart Cities. *Asian Journal for Convergence In Technology (AJCT)*, *8*(2), 45-50. ISSN-2350-1146.
- Pradhan, D., Tun, H. M., Wah, N. K. S., Oo, T., Priyanka, K. C., & Dash, A. (2022, July). Efficient Usage of Energy in 5G toward Sustainable Development inclined to Industry 4.0 Connectivity. In *2022 IEEE Region 10 Symposium (TENSYMP)* (pp. 1-6). IEEE.
- Priyanka, K., Mallavaram, G., Raj, A., Pradhan, D., & Rajeswari. (2022). Cognitiveness of 5G Technology Toward Sustainable Development of Smart Cities. *Decision Support Systems for Smart City Applications*, *20*, 189-203.
- Shivam, Y. (2021). A Detail Survey of Channel Access Method for Cognitive Radio Network (CRN) Applications toward 4G. *South Asian Res J Eng Tech*, *3*(1), 31-41.
- Singh, H. W., Devaki, K., Fernandes, J. V., & Pradhan, D. (2022, July). Pod vs SNR estimation: C-MIMO radar using STC and STAP algorithm. In *2022 IEEE Region 10 Symposium (TENSYMP)* (pp. 1-6). IEEE. doi: 10.1109/TENSYMP54529.2022.9864415.
- Srivastava, S., Rai, S., Kumar, S., Bhuhsan, S., & Pradhan, D. (2020). IoT based Human Guided Smart Shopping Cart System for Shopping Center. *Saudi Journal of Engineering and Technology*, *5*(6), 278-84.
- Tun, H. M., Nwe, M. S., Naing, Z. M., Latt, M. M., Pradhan, D., & Sahu, P. K. (2022). Research on Self-balancing Two Wheels Mobile Robot Control System Analysis. *Electrical Science & Engineering*, *4*(1), 7-20.
- Tun, H. M., Nwe, M. S., Naing, Z. M., Latt, M. M., Pradhan, D., & Sahu, P. K. (2022). Research on Self-balancing Two Wheels Mobile Robot Control System Analysis. *Electrical Science & Engineering*, *4*(1), 7-20.
- Wah, N. K. S. (2023). Integration of AI/Ml in 5G Technology toward Intelligent Connectivity, Security, and Challenges. *Machine Learning Algorithms and Applications in Engineering*, 239-245.