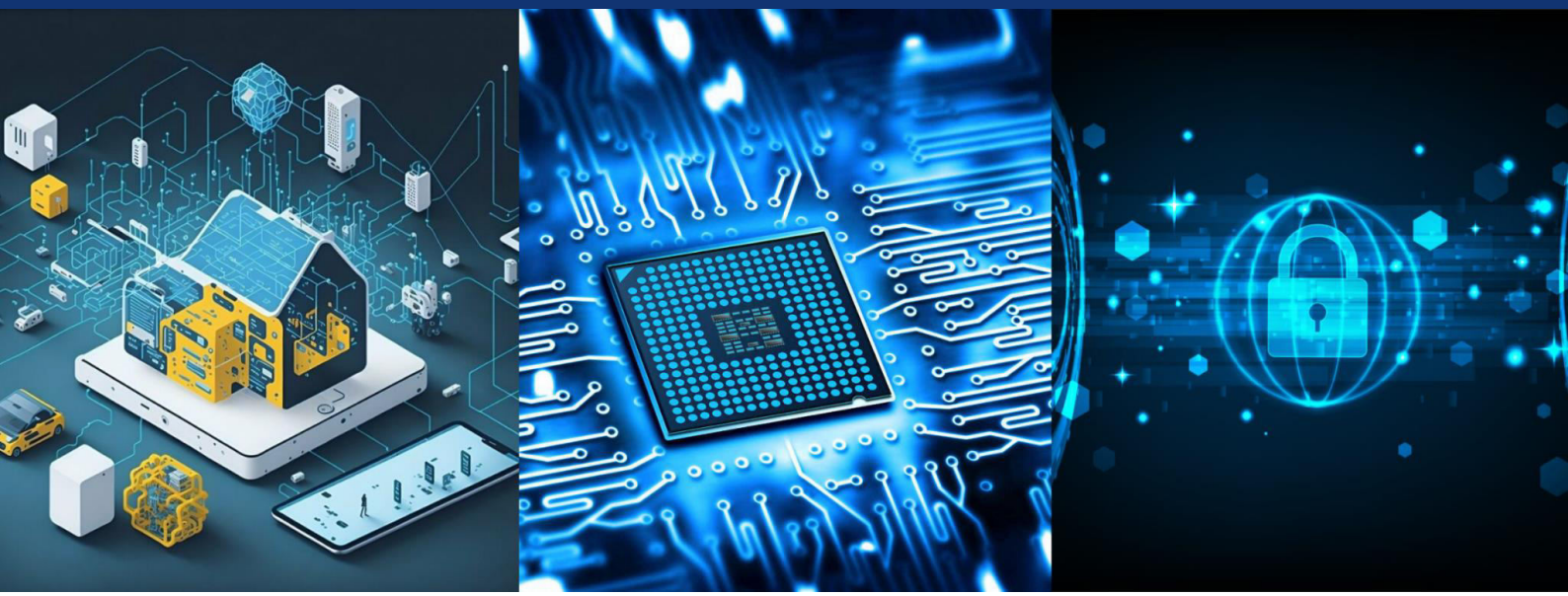
IJIRCCE

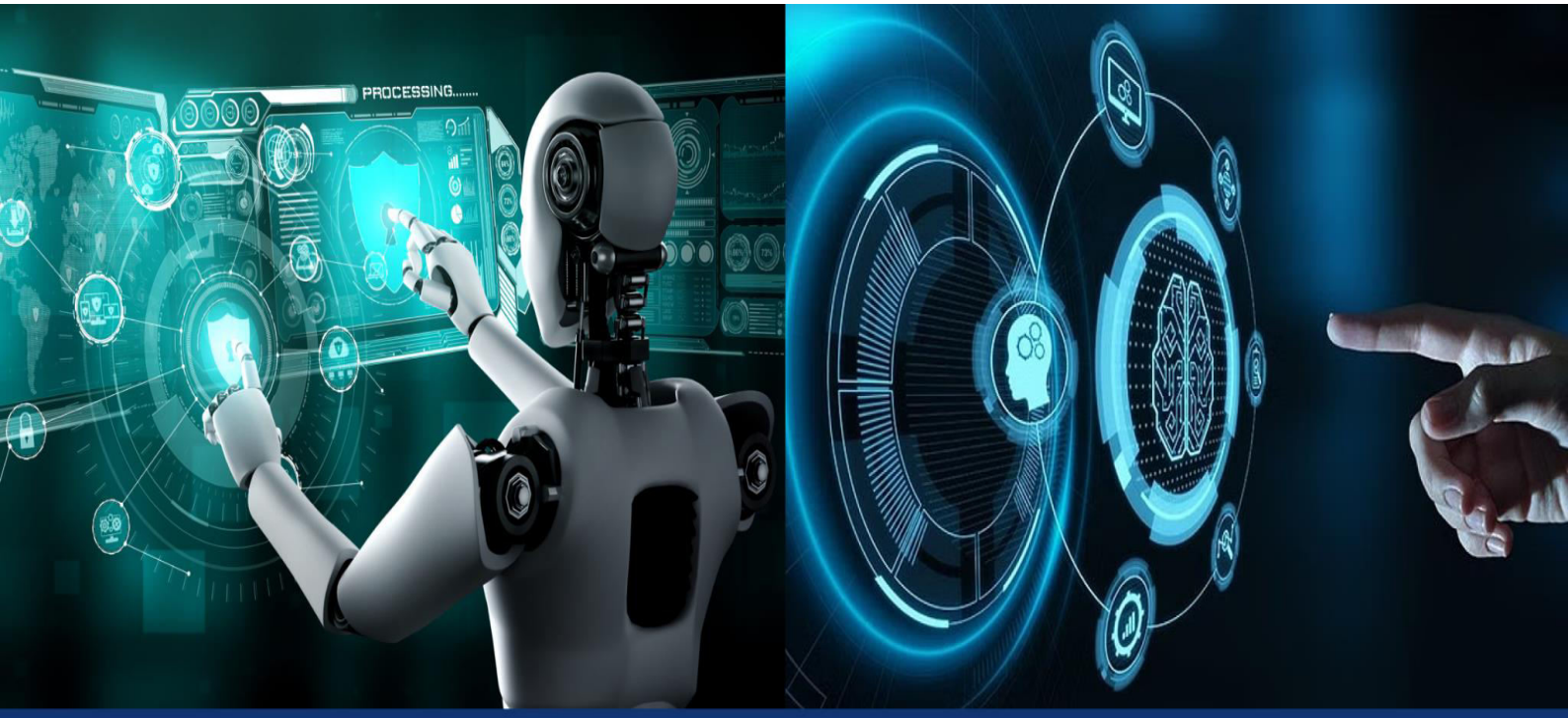
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407045

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Invisible Configuration Conflicts Detector Using Machine Learning a Random Forest–Based Intelligent Framework for Software Configuration Conflict Detection

Dr. T.V.S Sriram[1], Mr. RamKrishna[2], K. Manoj[3]

Sr. Asst. Professor, Dept. of MCA, NSRIT, Visakhapatnam, AP, India[1]

Asst. Professor, Dept. of MCA, NSRIT, Visakhapatnam, AP, India[2]

Dept. of MCA, NSRIT, Visakhapatnam, AP, India[3]

ABSTRACT: IoT-enabled cyber-physical systems are widely used in smart cities, industries, healthcare, and home automation because they improve efficiency and connectivity. However, these systems are highly vulnerable to cyber-attacks due to weak security mechanisms, limited device resources, and large-scale interconnected networks. Attacks such as DDoS, data injection, and malware can seriously affect system reliability and safety. Therefore, accurate and fast intrusion detection is essential for protecting IoT environments.

This project presents a hybrid deep learning framework for detecting security attacks in IoT-enabled cyber-physical systems. The proposed model combines two deep learning classifiers, **Convolutional Neural Network (CNN)** and **Deep Belief Network (DBN)**, to improve attack detection performance. To enhance classification accuracy, the model parameters are optimized using a novel hybrid metaheuristic optimization algorithm called **Seagull Adapted Elephant Herding Optimization (SAEHO)**, which integrates the strengths of Seagull Optimization and Elephant Herding Optimization for better exploration and exploitation.

The framework follows three main stages: preprocessing and normalization, feature extraction using statistical and higher-order statistical features, and final classification into attack or benign traffic. The proposed system is evaluated using two benchmark datasets, **UNSW-NB15** and **BoT-IoT**, and performance is measured using metrics such as accuracy, sensitivity, specificity, and precision. Experimental results show that the **Hybrid Classifier + SAEHO** approach achieves better detection accuracy and improved performance compared to conventional deep learning and optimization-based methods.

I. INTRODUCTION

The rapid growth of the **Internet of Things (IoT)** has transformed many real-world domains such as **smart cities, healthcare, smart homes, industrial automation, and transportation**. IoT devices are equipped with sensors, software, and network connectivity, which helps them collect, process, and share data automatically. Because of this, IoT systems improve efficiency, productivity, user experience, and resource management in modern society.

However, despite these advantages, **IoT-enabled Cyber-Physical Systems (CPS)** face serious security challenges. These systems are highly interconnected and often operate in complex and dynamic environments, making them more vulnerable to cyber-attacks. Many IoT devices also have **limited computational power**, which restricts the use of strong security mechanisms. As a result, attackers can exploit weak configurations and insecure communication to perform harmful activities such as **data injection, malware infections, and Distributed Denial of Service (DDoS)** attacks. Such attacks can damage system reliability and even threaten public safety.

To handle these challenges, an effective **attack detection model** is essential. Traditional security methods may not perform well in IoT-enabled CPS due to the unique nature of IoT traffic and resource constraints. Therefore, **Deep**

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Learning (DL) has become a strong solution for detecting cyber-attacks because it can automatically learn patterns from large-scale network data and classify traffic as **benign or malicious**.

II. LITERATURE REVIEW

IoT-enabled cyber-physical systems (CPS) are becoming common in smart cities, smart homes, healthcare, industrial automation, and other real-world applications. Even though these systems provide high connectivity and automation, they face serious security risks. Traditional security methods are not always effective in IoT environments because IoT devices have limited resources and generate huge network traffic. Due to this, researchers have started using machine learning (ML) and deep learning (DL) methods for intrusion detection and attack classification.

Mohamed et al. (2023) studied the use of machine learning in IoT-based smart systems such as smart cities and smart campuses. They categorized ML techniques into linear and non-linear models and explained how these models can help in securing IoT networks. Their work also discussed evaluation metrics and the importance of selecting suitable ML models for smart IoT systems.

Pedro et al. (2023) focused on intrusion detection in industrial IoT using federated learning. Their work mainly targeted privacy-preserving intrusion detection by applying differential privacy and noise addition methods. They tested their approach using the ToN_IoT dataset and showed that federated learning can protect privacy while maintaining good accuracy. This study highlighted the importance of privacy and secure distributed training in IoT environments.

III. SYSTEM OVERVIEW

The proposed system is designed to detect and classify security attacks in **IoT-enabled Cyber-Physical Systems (CPS)** using a **Hybrid Optimization Algorithm** integrated with Machine Learning. The system continuously monitors network traffic and sensor data collected from IoT devices deployed in a cyber-physical environment. After collecting the data, preprocessing techniques such as data cleaning, normalization, and feature selection are applied to improve data quality.

A hybrid optimization algorithm is then used to identify the most relevant features and optimize the machine learning model for improved attack detection performance. The optimized model is trained to recognize both normal and malicious activities, enabling accurate detection of various cyber-attacks such as Denial of Service (DoS), Distributed DoS (DDoS), spoofing, and intrusion attacks.

When new data is received from IoT devices, the trained model analyzes it in real time and classifies it as either normal or an attack. If an attack is detected, the system immediately generates an alert, allowing administrators to take preventive actions. This approach enhances detection accuracy, reduces false alarms, and improves the overall security and reliability of IoT-enabled Cyber-Physical Systems.

IV. METHODOLOGY

Data Collection: Collect IoT network traffic and sensor data containing both normal and attack records.
Data Preprocessing: Clean the data, remove missing values, normalize features, and encode categorical data.
Hybrid Optimization: Apply a hybrid optimization algorithm to select the most important features and improve model performance.
Model Training: Train the machine learning model using the optimized dataset.
Attack Detection: Classify incoming data as **Normal** or **Attack** in real time.
Alert Generation: Generate alerts when malicious activities are detected and evaluate the model using accuracy, precision, recall, and F1-score..

V. SYSTEM ARCHITECTURE

Algorithm for detecting security attacks in IoT-enabled Cyber-Physical Systems. The process begins with **data collection**, where network traffic and sensor data are gathered from IoT devices. The collected data is then sent to the **data preprocessing** stage, where it is cleaned, normalized, and prepared for analysis. Next, multiple **machine learning algorithms** such as Logistic Regression (LR), Random Forest (RF), Decision Tree (DT), Extra Trees (ET), K-Nearest

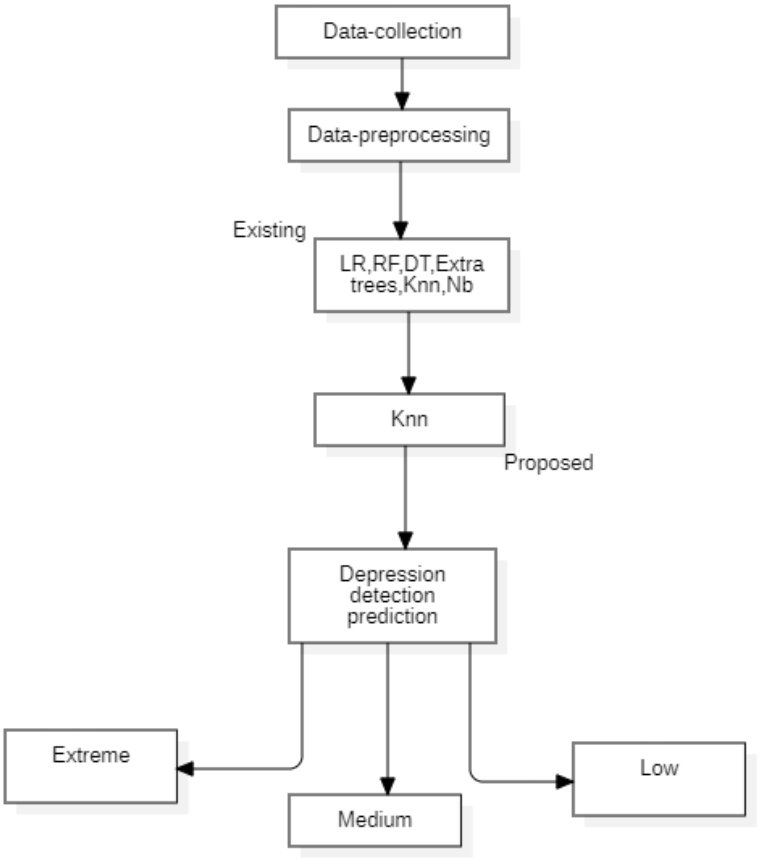
© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407045

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Neighbors (KNN), and Naïve Bayes (NB) are trained and evaluated. Based on their performance, the **best model** is selected. The selected model is then used for **security attack detection**, where incoming data is classified as either **Normal Traffic** or **Attack Detected**. If an attack is identified, the system generates an alert, enabling administrators to take timely security



VI. MODULES

The proposed system consists of the following modules:

6.1 Data Collection Module

This module collects network traffic and sensor data from IoT-enabled Cyber-Physical Systems. The collected dataset contains both normal and malicious network activities, which are used for model training and testing.

6.2 Data Preprocessing Module

The collected data is cleaned by removing duplicate records and handling missing values. Data normalization, feature encoding, and transformation techniques are applied to prepare the dataset for machine learning.

6.3 Hybrid Optimization Module

This module applies a hybrid optimization algorithm to select the most relevant features from the dataset. Feature selection improves model accuracy, reduces computational complexity, and enhances detection efficiency.

6.4 Machine Learning Module

Multiple machine learning algorithms are trained using the optimized dataset. Their performance is evaluated, and the best-performing model is selected for security attack detection.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

6.5 Attack Detection Module

The trained model analyzes incoming IoT network traffic and classifies it as either **Normal** or **Attack**. The system detects various cyber-attacks with high accuracy.

6.6 Alert and Monitoring Module

When malicious activity is detected, the system immediately generates an alert for the administrator. This module supports continuous monitoring and helps prevent security threats.

6.7 Database Module

The database stores network traffic records, processed data, prediction results, and attack logs for future analysis and monitoring.

VII. IMPLEMENTATION DETAILS

7.1 Technology Stack

The proposed system is developed using **Python** for programming and machine learning implementation. The **Scikit-learn** library is used for model development, while **Pandas** and **NumPy** are used for data preprocessing. The system is implemented using **Jupyter Notebook/Google Colab**, and datasets are stored in **CSV** format.

7.2 Data Preprocessing

The dataset undergoes data cleaning, missing value handling, duplicate removal, normalization, and feature encoding. Hybrid optimization is then applied to identify the most significant features for attack detection.

7.3 Hybrid Optimization Implementation

The hybrid optimization algorithm performs feature selection by identifying the optimal feature subset, reducing redundant information, and improving machine learning performance.

7.4 Machine Learning Model

Multiple machine learning algorithms such as **Logistic Regression, Random Forest, Decision Tree, Extra Trees, K-Nearest Neighbors, and Naïve Bayes** are trained and tested. The best-performing model is selected based on evaluation metrics.

7.5 Attack Detection

The trained model analyzes incoming IoT network traffic and predicts whether the activity is **Normal** or **Attack**. The prediction results are generated in real time.

7.6 Security Measures

The system ensures data integrity through preprocessing, optimized feature selection, and accurate attack classification. Alert generation helps administrators respond quickly to detected threats.

VIII. EXPERIMENTAL DETAILS AND RESULTS

8.1 Experimental Setup

The proposed system was implemented using Python, Scikit-learn, Pandas, NumPy, and Google Colab/Jupyter Notebook. The model was trained and tested using an IoT cybersecurity dataset containing normal and attack traffic. Performance was evaluated using standard classification metrics.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407045

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

8.2 Test Results

Test Case	Description	Result Status
Data Collection	Collect IoT network traffic	Passed ✓
Data Preprocessing	Clean and normalize dataset	Passed ✓
Feature Selection	Apply Hybrid Optimization	Passed ✓
Model Training	Train machine learning model	Passed ✓
Attack Detection	Detect security attacks	Passed ✓
Alert Generation	Generate attack alerts	Passed ✓

8.3 Performance Evaluation

The hybrid optimization-based machine learning model successfully detected cyber-attacks with high prediction accuracy. Feature optimization improved classification performance while reducing computational complexity. The system efficiently classified both normal and malicious network traffic.

8.4 Observations

The proposed system successfully identified security attacks in IoT-enabled Cyber-Physical Systems with improved detection accuracy. Hybrid optimization reduced irrelevant features, resulting in faster processing and more reliable attack detection. The system demonstrated efficient performance during testing.

IX. APPLICATIONS

The proposed **Hybrid Optimization Algorithm for Detection of Security Attacks in IoT-Enabled Cyber-Physical Systems** can be applied in:

- IoT Network Security
- Smart Cities
- Industrial Control Systems (ICS)
- Smart Grid Security
- Healthcare IoT Systems
- Smart Home Automation
- Cloud-Based IoT Platforms
- Cybersecurity Monitoring Centers
- Research and Academic Studies
- Real-Time Intrusion Detection Systems

X. LIMITATIONS

The proposed system has the following limitations:

- Prediction accuracy depends on the quality of the training dataset.
- The system supports only known attack patterns included in the dataset.
- Real-time deployment requires high computational resources.
- New attack types may require retraining of the machine learning model.
- Performance may decrease with extremely large-scale IoT environments.
- The effectiveness of feature selection depends on the chosen hybrid optimization technique.

XI. FUTURE ENHANCEMENTS

The proposed system can be improved by:

- Implementing deep learning models for higher detection accuracy.
- Supporting real-time IoT network monitoring.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

- Integrating cloud and edge computing environments.
- Detecting zero-day and unknown cyber-attacks.
- Developing a web-based dashboard for attack visualization.
- Supporting large-scale distributed IoT networks.
- Applying advanced hybrid optimization techniques.
- Enhancing automatic response and threat mitigation mechanisms.

XII. CONCLUSION

The Hybrid Optimization Algorithm for Detection of Security Attacks in IoT-Enabled Cyber-Physical Systems provides an intelligent solution for identifying cyber threats in IoT networks. By combining hybrid optimization with machine learning, the system effectively selects relevant features and accurately detects malicious activities. The proposed approach improves detection accuracy, reduces computational complexity, and supports efficient cybersecurity monitoring.

Experimental results demonstrate that the proposed system successfully classifies normal and attack traffic with high performance. Overall, the project highlights the effectiveness of hybrid optimization and machine learning in securing IoT-enabled Cyber-Physical Systems and provides a strong foundation for future research and real-time deployment.

REFERENCES

[1] K. Min, J. Yoon, M. Kang, D. Lee, E. Park, and J. Han, “Detecting depression on video logs using audiovisual features,” no. 2023, doi: 10.1057/s41599-023-02313-6.
[2] H. Zhang, H. Wang, S. Han, W. Li, and L. Zhuang, “Computer Methods and Programs in Biomedicine Detecting depression tendency with multimodal features,” Comput. Methods Programs Biomed., vol. 240, no. January 2022, p. 107702, 2023, doi: 10.1016/j.cmpb.2023.107702.
[3] J. Jovel, R. Greiner, and R. Greiner, “An Introduction to Machine Learning Approaches for Biomedical Research,” vol. 8, no. December, pp. 1–15, 2021, doi: 10.3389/fmed.2021.771607.
[4] J. Maurya and S. Prakash, “Heart Disease Prediction and Diagnosis Using IoT, ML, and Cloud Computing,” in International Conference on Innovative Computing and Communications, A. E. Hassanien, O. Castillo, S. Anand, and A. Jaiswal, Eds., Singapore: Springer Nature Singapore, 2024, pp. 419–430.
[5] I. Conference, “Feature Selection and Imbalanced Data Handling for Depression Detection : Feature Select ion and Imbalanced Data Handling for Depression Detection,” no. September 2023, 2018, doi: 10.1007/978-3-030-05587-5.
[6] R. Islam, M. A. Kabir, A. Ahmed, A. R. M. Kamal, and H. Wang, “Depression detection from social network data using machine learning techniques,” Heal. Inf. Sci. Syst., vol. 6, no. 1, pp. 1–12, 2018, doi: 10.1007/s13755-018-0046-0.
[7] H. Alsagri, “Machine Learning-based Approach for Depression Detection in Twitter Using Content and Activity Features,” vol. 1, pp. 1–16.
[8] A. Ahmed, R. Sultana, M. T. R. Ullas, M. Begom, M. M. I. Rahi, and M. A. Alam, “A Machine Learning Approach to detect Depression and Anxiety using Supervised Learning,” 2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020, pp. 4–9, 2020, doi: 10.1109/CSDE50874.2020.9411642.
[9] S. J. T. J, I. J. Jacob, and A. K. Mandava, “D-ResNet-PVKELM : deep neural network and paragraph vector based kernel extreme machine learning model for multimodal depression analysis,” pp. 25973–26004, 2023.
[10] D. Kumar, U. Subrajeet, M. Niraj, and K. Singh, “An early assessment of Persistent Depression Disorder using machine learning algorithm,” Multimed. Tools Appl., no. 0123456789, 2023, doi: 10.1007/s11042-023-17369-4.
[11] D. Pokrajac, “The successful discrimination of depression from EEG could be attributed to proper feature extraction and not to a particular classification method,” vol. 0123456789, pp. 443–455, 2020, doi: 10.1007/s11571-020-09581-x.
[12] A. Albtoush and M. Ferna, “Quick extreme learning machine for large-scale classification,” vol. 8, pp. 5923–5938, 2022, doi: 10.1007/s00521-021-06727-8.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

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