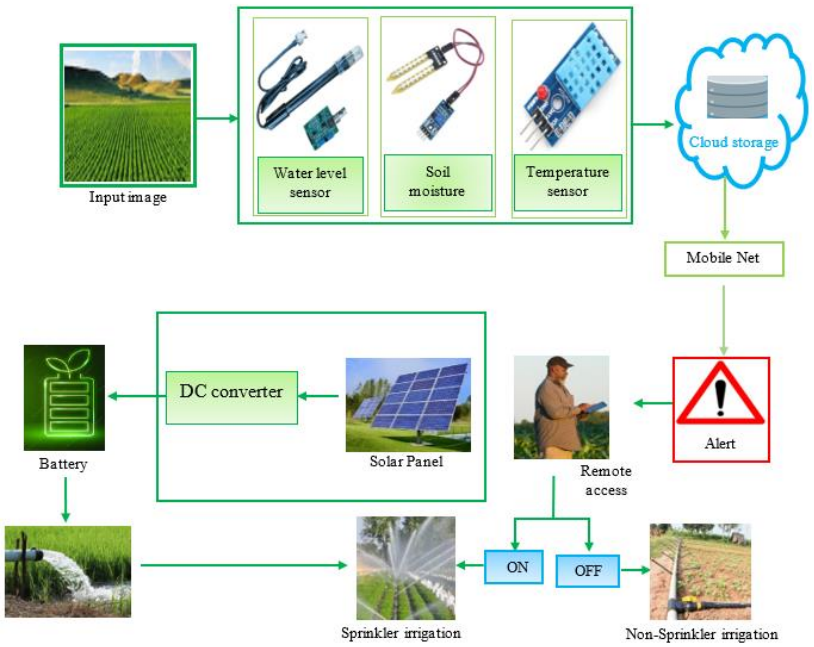
IJCEO

International Journal of Computer and Engineering Optimization

1. SMART AGRICULTURE IN SPRINKLER IRRIGATION USING DEEP LEARNING NETWORK

Amudaria S, Joseph Jawhar S

ABSTRACT: An Internet of Things (IoT) is used to provide information about agricultural areas and then take action based on user input in "smart agriculture," an emerging idea. In this paper, a novel Smart agriculture based on Solar panel for Sprinkler irrigation (SSS) system that collects and monitors the environmental temperature, soil moisture and humidity. The temperature, humidity, and soil moisture measurements are kept in the cloud for analysis. Data obtained from cloud storage is validated by MobileNet. A farmer receives an alarm message from the mobile net if the soil moisture content is less than 20%, if the temperature and humidity are less than -40°C to +80°C, and if the relative humidity is between 0% and 100%. A mobile net alarm message is sent to a farmer if the pH is lower than 5.5. Solar panels are the renewable energy source for the farm and battery. When needed, the water pumps are powered by the element that stores extra electrical energy produced by the solar panels. A farmer uses sprinkling irrigation to remotely access the field after receiving an alert message from the mobile network. A farmer can remotely access a field and irrigate a farm using sprinkler irrigation when they receive an alarm message from the mobile network. The proposed method improves the overall accuracy of 98.57%, 96.24%, 89.65%, 91.68% and 99.37% AlexNet, ResNet-50, DenseNet, GoogleNet and MobileNet respectively.

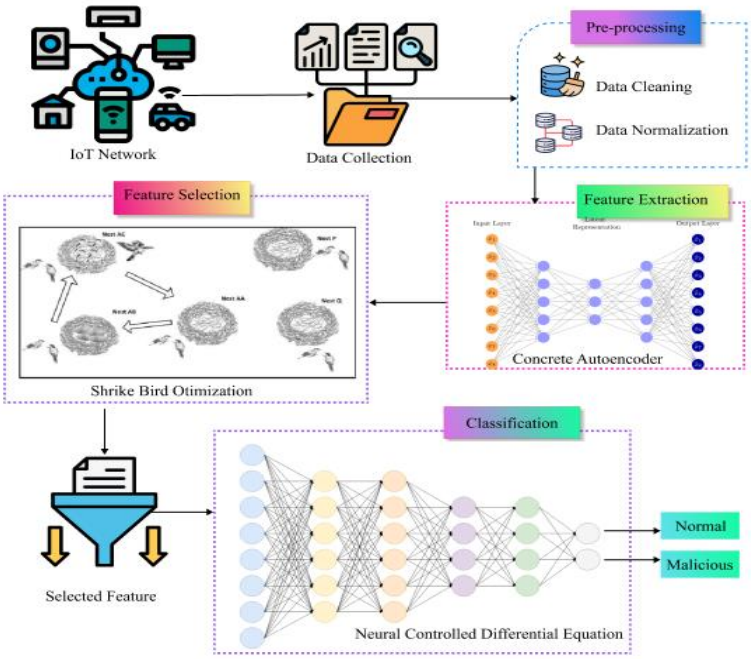


Keywords – *Deep learning, DC converter, sprinkler irrigation.*

2. SOAL-IOT: SHRIKE BIRD OPTIMIZATION AND CONCRETE AUTOENCODER BASED DEEP LEARNING FRAMEWORK FOR IOT INTRUSION DETECTION

Sandhya M, Aisha Banu W, Leninisha Shanmugam, Arputha Rathina X

Abstract: The Internet of Things (IoT) consists of interconnected devices that continuously exchange data, making security a critical concern. However, a number of issues pertaining to IoT security and privacy have emerged as a result of its broad use. For IoT-enabled services to be dependable, secure, and profitable, real-time intrusion detection on IoT devices is essential. Current Intrusion Detection Systems (IDSs) frequently face challenges such as a high False Alarm Rate (FAR), mean squared error, and reduced intrusion detection reliability and accuracy. To address intrusion detection challenges in IoT environments, this work proposes the Shrike bird Optimization and concrete Autoencoder-based deep Learning framework for IOT intrusion detection (SOAL-IOT), as illustrated in the diagram. The process begins with IoT network traffic collection, followed by data pre-processing, which integrates data cleaning and normalization to improve high-quality data. Then, Feature Extraction (FE) is performed using a Concrete Autoencoder (CAE) to learn compact and meaningful feature representations. The extracted features are then refined through Shrike Bird Optimization (SBO) for effective feature selection, which reduces redundancy and computational complexity. Finally, the selected features are classified using a Neural Controlled Differential Equation (NCDE)-based model to accurately distinguish between normal and malicious traffic. Experimental findings on the BoT-IoT datasets demonstrate that the proposed model improves overall accuracy by 4.93%, 6.26% and 4.23% over SPOHDL-ID, CST-AFNet, and HIDSIoMT on the BoT-IoT Dataset.

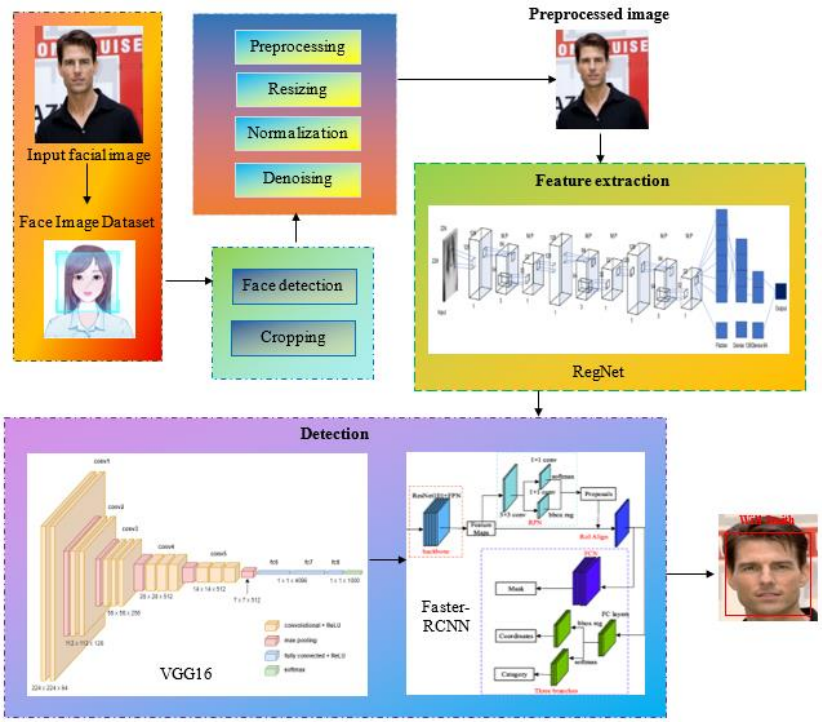


Keywords – *Intrusion Detection, Shrike Bird Optimization, Deep Learning, Neural Controlled Differential Equation, Internet of Things.*

3. FA-FAS NET: DEEP LEARNING NETWORK FOR FACE RECOGNITION USING FASTER REGION BASED CONVOLUTIONAL NEURAL NETWORK

Kiruba Jothi D, Ashok Y

Abstract: Face recognition (FR) has become an essential biometric technology for security, surveillance, and identity verification in modern intelligent systems. However, existing FR approaches often suffer from reduced accuracy under challenging conditions like pose variation, illumination changes, occlusion, and background noise. To address these limitations, a novel FA-FAS Net is proposed for robust and accurate face recognition. the input facial image is obtained from a face image dataset and passed through a face detection and cropping stage to isolate the facial region from the background. The detected face fed into preprocessing, it includes resizing to a standard dimension, normalization to maintain consistent pixel intensity distribution, and denoising to remove unwanted noise and enhance image quality. The pre-processed image is subsequently forwarded to the feature extraction module, where a deep convolutional neural network based on RegNet is employed to learn discriminative facial representations and generate robust feature maps. These extracted features are then utilized in the detection and recognition stage, where a backbone network inspired by VGG16 supports the object detection framework implemented using Faster R-CNN, which accurately localizes and classifies the detected face. Finally, the system outputs the recognized identity, demonstrating the efficiency of the integrated deep learning framework for reliable and high-precision FR in real-world applications. The FA-FAS Net maintains high accuracy levels of 98.87% based on the gathered dataset. The FA-FAS Net enhances the total accuracy by 0.99%, 4.07% and 4.92% better than FER, CNN, and Deep neural network respectively.

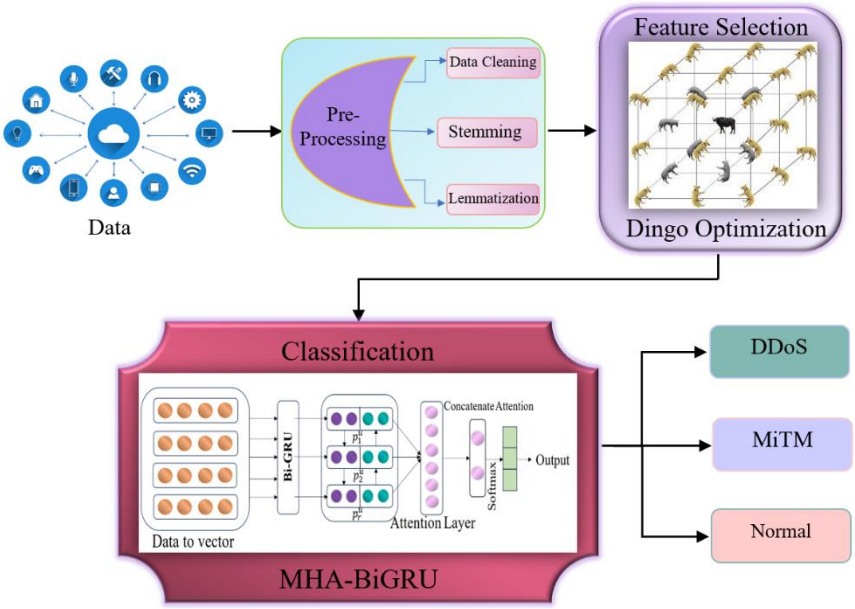


Keywords *– Face Recognition, Deep Learning, Attention Mechanism, Feature Fusion, Biometric Identification, Image Classification.*

4. REAL-TIME INTRUSION DETECTION IN IOT WITH DEEP LEARNING-BASED MULTI-HEAD ATTENTION BIGRU

Christal Anto V, Ahilan A

Abstract: The Internet of Things (IoT) links a wide range of physical devices to the Internet, facilitating cutting-edge applications in fields like the military, healthcare, agriculture, and transportation. These IoT applications have grown in popularity due to their ability to tackle real-time challenges effectively. However, despite the benefits they provide IoT systems are notably susceptible to security vulnerabilities, making them targets for a range of cyberattacks. These threats include DDoS, MiTM, sinkhole attacks, eavesdropping, and DoS attacks. In this work, a novel Real-Time Intrusion Detection in IoT with a Deep Learning-based Multi-Head Attention BiGRU (RIGRU) approach has been proposed to accurately classify IoT attacks. Data is collected from IoT sensors on network devices. It goes through data cleaning and standardization. Dingo Optimization is used to select relevant features iteratively for classification tasks. These features are then fed into a Multi-Head Attention BiGRU Network to detect MiTM, DDoS attack and normal. The proposed RIGRU approach was calculated utilizing various metrics, namely precision, f1score, recall, and accuracy. The RIGRU model advances the overall accuracy by 0.87%, 0.95%, and 0.75%, over the PCC-CNN, DIDS and GNN, respectively.



Keywords – *Deep Learning, Dingo Optimization Algorithm, Intrusion Detection, Internet of Things.*