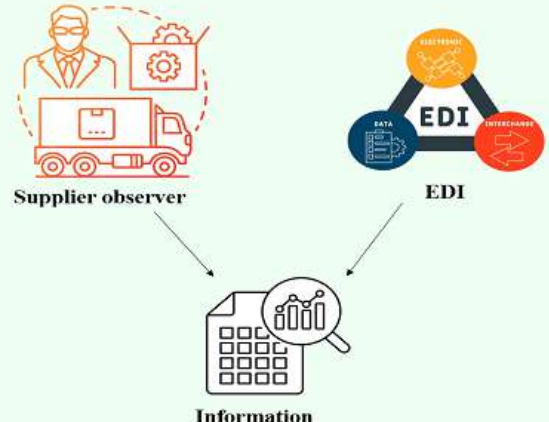
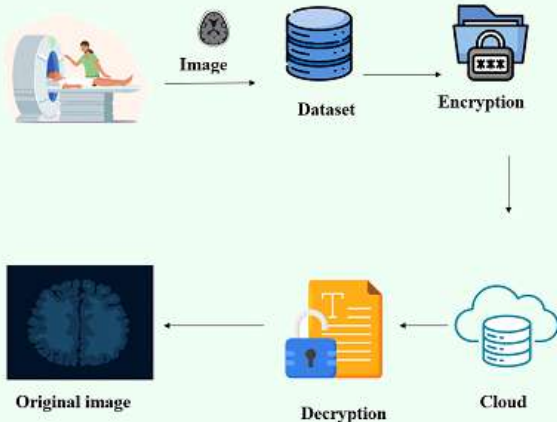
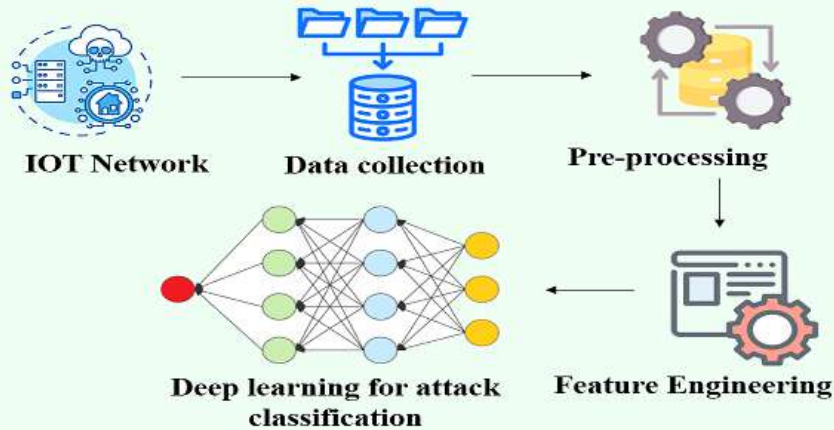
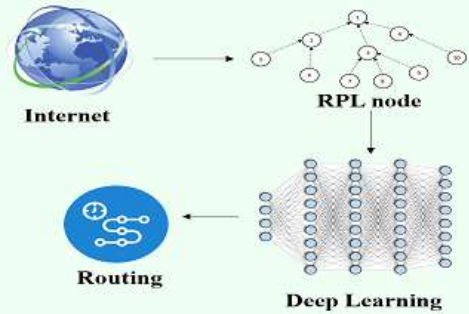
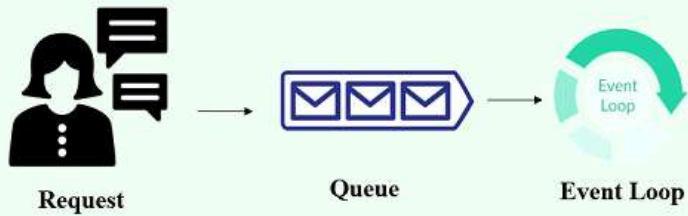


IJCEO

ISSN: XXXX - XXXX

International Journal of Computer and Engineering Optimization

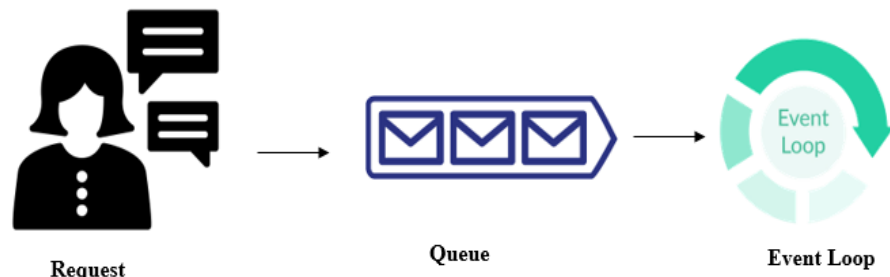


International Journal of Computer and Engineering Optimization IJCEO

1. ENHANCING CONVERSATIONAL INTERFACES: A REACT AND LLM-BASED APPROACH TO WEBSOCKET CHATBOT APPLICATIONS

Reshmi Tatikonda

Abstract – Chatbots have become integral to modern digital communication, particularly in industries like Retail, Supply Chain, and E-Commerce, where seamless interaction is key to customer



satisfaction. This paper presents the design, development, and implementation of a WebSocket-based chatbot application that combines responsive front-end technologies with the advanced capabilities of large language models (LLMs). Leveraging React, JavaScript, HTML, and CSS, the chatbot interface ensures an intuitive and dynamic user experience while WebSocket facilitates real-time communication. By integrating LLMs, the chatbot enhances its ability to interpret user queries, deliver personalized responses, and transition to live agents when necessary. Comprehensive performance evaluation and user satisfaction metrics highlight the system's efficiency and accuracy. This research contributes to advancing chatbot design by integrating emerging technologies for seamless conversational experiences. User feedback indicated a high level of satisfaction with the system, with 92% of users reporting a positive experience. The combination of real-time interactions and accurate responses contributed to this outcome, with a 95% intent recognition accuracy achieved by the LLM-powered system.

Keywords – Chatbot, WebSocket, React, User Experience, Real-Time Communication, Artificial Intelligence.

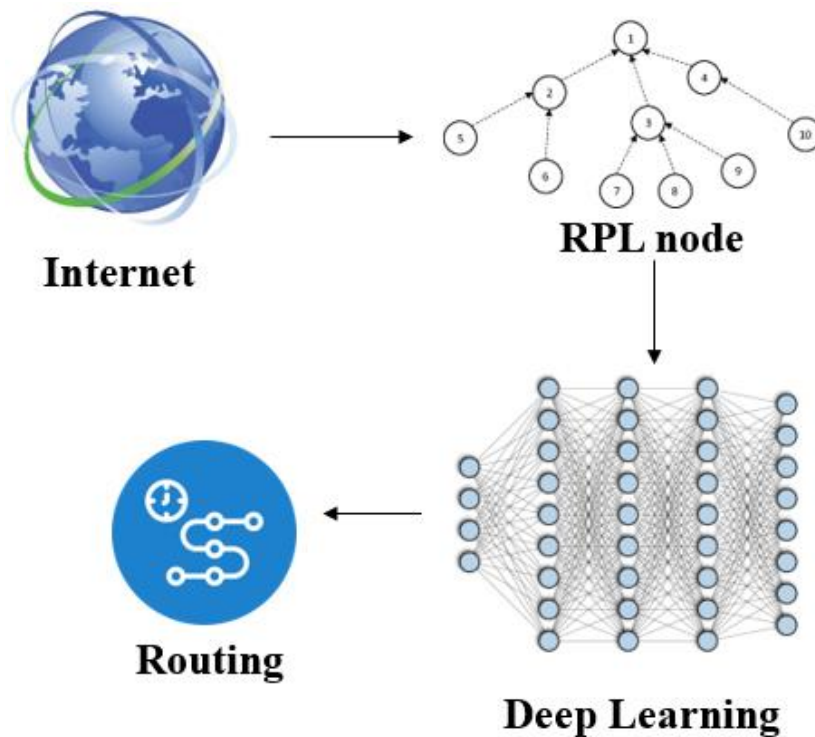
2. DARE-RPL DEEP SEQUENTIAL NEURAL NETWORK BASED AUTHENTICATED ROUTING IN RPL

S.V. Thilagan

Abstract – The Internet of Things has been heralded as the most important technical development in recent years due to its low-cost and low-power sensor technology. The IoT makes everyday tasks easier, including smart transportation, smart housing, and smart healthcare, which uses Bluetooth and other low-power wireless technologies in low power lossy network (LLN). The LLN has low throughput and substantial delay due to its traffic patterns, to communicate with resource-constrained sensor devices. To fix this issue RPL is used to solve

complicated problems. Routing Protocol for Low-Power and Lossy Networks (RPL) is still working through issues with energy use, scalability, security, and dependability, to name just a few. However, managing all of these challenges in the RPL-IoT network is essential since the RPL contains heterogeneous traffic. In this paper, a novel approach on Deep Sequential Neural Network (DSNN) based Authenticated Routing Enforced RPL (DARE-RPL) is introduced to overcome complex issues in routing and secure transmission of packet. The border router for the LLN network additionally connects the roots to the internet. It has been suggested to use a secure RPL with a congestion avoidance approach to lessen traffic and offer a secure environment. DSNN is the congestion detection method used to avoid congestion in the network during the transmission. The MATLAB simulator is use to evaluate the DARE-RPL technique. The load balancing capacities of the RPI-IOT and MADM current systems are lower for the same set of malicious nodes, at 69% and 58%, respectively, compared to the 93% load balancing capacity achieved by our proposed DARE-RPL.

Keywords – Routing Protocol for Low-Power and Lossy Networks, Deep Sequential Neural Network, Congestion, Internet of Things.



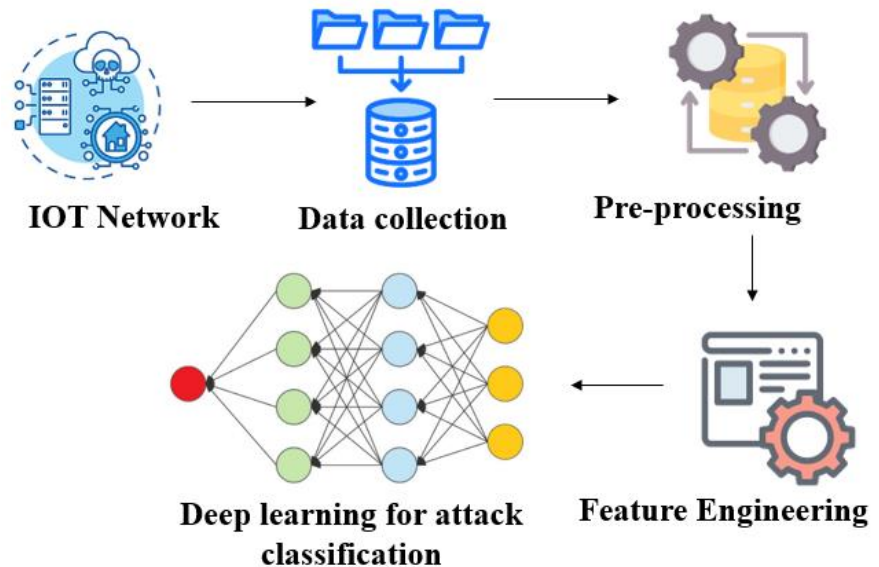
3. HYBRID GRAPH BASED CONVOLUTIONAL NEURAL NETWORK FOR INTRUSION DETECTION IN IOT

Vishnu Karthik Ravindran

Abstract – Cyberattacks on critical Internet of Things (IoT) systems must be detected using Intrusion Detection Systems (IDS). It is necessary to enhance the protection of these devices from cyberattacks in order to safeguard their users. A common feature of IDSs' anomaly detection components is deep learning (DL) techniques. ML approaches have been used for many years to

increase the reliability and resilience of Network Intrusion Detection Systems (NIDS). In the last few years, to identify intrusions in the Internet of Things (IoT), deep learning algorithms are employed. Intrusion is one of the major issues in IOT due to lack of security, attacks on network, accuracy etc., in the network. In order to overcome this problem, a novel Hybrid Convolutional neural network and Graph convolutional network (CNN-GCN) technique has been proposed in this work for IOT intrusion detection. The proposed CNN-GCN deals with attacks issue on network, accuracy rate and lack of security in IOT. The proposed work improves feature extraction, accuracy and attention-based classification. Performance evaluation of the suggested method will be done using the MATLAB simulator. The proposed technique performance has been assessed using specific metrics such as accuracy, classification and error detection. In comparison to the existing methods, the findings demonstrate that the proposed work exhibits 99.86% error detection in IOT.

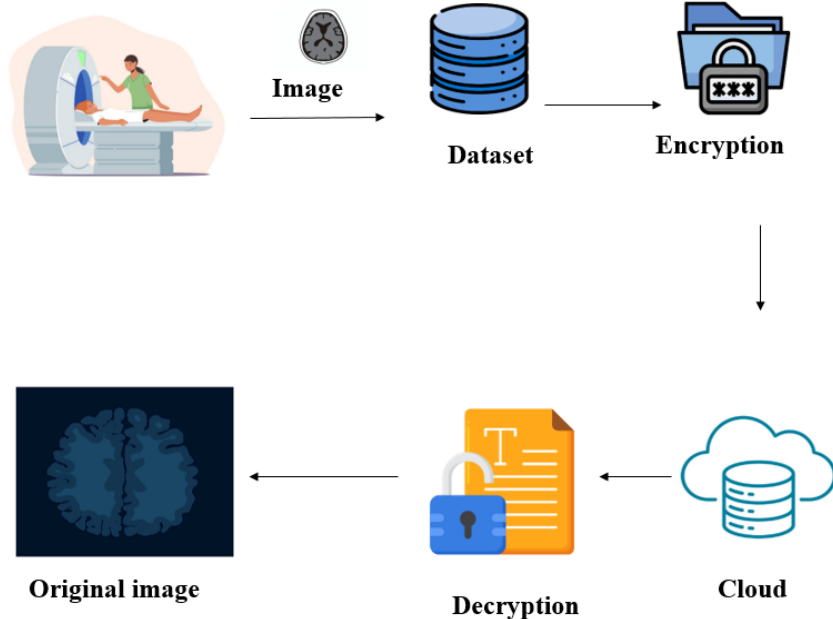
Keywords – Cyberattacks, Internet of Things, Convolutional neural network, Graph convolutional network.



4. CROW SEARCH OPTIMIZED DNA ENCRYPTION FOR SECURE MEDICAL DATA TRANSMISSION

Hari Krishna Kalidindi

Abstract – Smart healthcare has become more and more popular as information technology has developed. In the contemporary information era, smart healthcare makes healthcare more efficient, convenient, and customized by completely changing the traditional medical system. Even if there are many ways that these advancements improve people's lives, one of the main concerns is still the security of the vast data transmission. In order to solve this issue, a novel



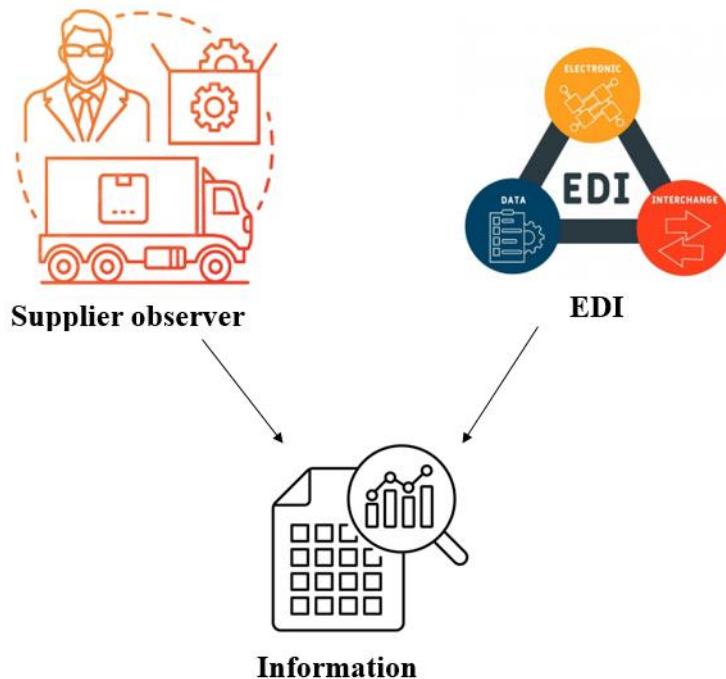
approach on Crow search optimized DNA encryption for SEcure medical data Transmission (CD-SET), for secure data transmission through unsecure channel is introduced in this paper. The proposed CD-SET model enhances the data transmission security by employing robust cryptographic techniques while transmitting through an unsecure channel. Initially medical image input is given to the encryption algorithm which combines DNA encryption and homomorphic encryption. The data will be first encrypted using DNA sequencing based on the sequence of the four chemical bases such as A, C, G, and T that comprise DNA. The DNA sequencing is given as input for HE Encryption process in which the key generation is performed using crow search algorithm. Then, the cloud stores the encrypted data so that it can be accessed. Python simulator is used to evaluate the proposed technique. The efficiency has been evaluated using encryption, decryption and execution time with the existing technique. The recommended technique can be implemented in 3% less time with the Dynamic DNA encryption system and Cryptosystem using SHA-512 algorithm and 7% less time with the Robust S-Box building method algorithm.

Keywords – Homomorphic algorithm, crow search optimization, encryption, decryption, data transmission.

5. BENEFITS OF WALMART'S ELECTRONIC DATA INTERCHANGE SYSTEM AND RESOURCE PLANNING MECHANISM FOR SUPPLIERS

Ramya Thatikonda

Abstract – This study examines a model of SC contracting involving a procurer seeking to obtain as much merchandise as possible at the lowest price. The supplier in this model possesses secluded statistics regarding its limited production capacity. Two information-sharing models are compared. The first one is where the supplier observes its capacity and reports it to the purchaser for committing to a purchase. This is referred to as the "Supply Chain" contract. The second model is; the purchaser directly hooks up with the supplier's Enterprise Resource Planning system with EDI. This eliminates information asymmetry. This is called the "Full Information"



contract. Although more economically efficient, suppliers may not want to accept the Full Information contract, since they would fear threats over profit margins or loss in control over sensitive information. The proposed third contract is termed as the "Hybrid" contract. This contract gives the buyer all the efficiency gains of the Full Information contract and yet ensures the supplier gets the same profits as with the Supply Chain contract. Although these benefits make the Hybrid contract preferable to the Full Information (FI) contract in its cost, the buyer will still prefer the Full Information contract over the Hybrid contract. A new level of complexity arises if the supplier can invest to expand capacity. It can be inferred that if the Hybrid contract encourages higher investment, then, depending on the level of information asymmetry not being extremely high, the buyer will also eventually want to choose Hybrid over the Full Information contract.

Keywords – Supply Chain Contract, Full Information Contract, Hybrid Contract, Information Asymmetry, Electronic Data Interchange (EDI), Capacity Investment, Supplier Profitability.