Journal of Computers Vol. 36 No. 1, February 2025, pp. 285-298
https://doi.org/10.63367/199115992025023601019

Integrating Convolutional Neural Network and Deep-Q-Network for the Performance Enhancement of Internet of Robotic Things

Yu-Ge Liu[1] and Bin-Feng Tang[2*]

[1] College of Urban Rail Transit and Information Technology, Liuzhou Railway Vocational Technical College, Liuzhou Guangxi 545616, China
rico-penny@ltzy.edu.cn

[2] Railway Communication and Signal College, Liuzhou Railway Vocational Technical College, Liuzhou Guangxi 545616, China
tangbf@ltzy.edu.cn

Received 22 March 2024; Revised 23 July 2024; Accepted 8 August 2024

Abstract. The Internet of Robotic Things (IoRT) plays an important role in various applications that help to make effective communication circumstances. However, the robots require the proper features about particular scenarios to make a clear decision. In addition, the system's security, robustness and flexibility are difficult to maintain while analyzing various robotic application-related scenarios. The difficulties are addressed using integrated techniques such as Convolution Neural Networks (CNN) and Deep Q Networks (DQN) to improve the overall robotic performance, such as object identification and abnormal behaviour prediction. Initially, various scenarios of visual information are collected with the help of the camera. The gathered information is processed using a convolution kernel and pooling layer for downsampling and extracting the features. The derived hierarchical features are utilized to observe the scenario and identify the objects. The extracted features are fed into the DQN approach, which utilizes the rewards in the reinforcement learning process to improve decision-making efficiency. The decisions generated are used to fine-tune robotic performance in different applications. Then, the system's efficiency is evaluated in various real-time application scenarios in which the IoRT system attains high robustness, security, flexibility, and reliability.

Keywords: internet of robotic things, sensor, convolutional neural network, deep-Q-network, robustness and reliability

1 Introduction

The Internet of Robotic Things (IoRT) [1] is the combination of robotics [2] and the Internet of Things (IoT) [3]. Robots are connected to the Internet for effective communication, automation, and collaboration. The IoRT has several key concepts, such as connectivity, sensor integration, collaboration, security, and privacy [4]. The IoRT connects robots to the Internet to make ships, command, instruct, and collect information. The IoRT interconnected robots are effectively utilized for control and flung monitoring that helps to maximize the robot's performance and abilities [5]. Then, the IoRT enables sensor integrations like cameras, contact sensors, microphones, and various environments. Incorporating sensors enables robots to establish connections and identify their surroundings, enhancing the informed choices available to them [6].

Furthermore, with IoRT, robots can carry out automated motion according to the specified parameters. Robot autonomy movements are efficiently employed in several areas, such as agriculture, healthcare, logistics, and manufacturing [7]. The IoRT system ensures the coordination and cooperation between humans and robots, which helps to meet the objectives in various applications. In addition, the IoT-enabled robotic process provides various knowledgeable information that makes effective decisions in a decentralized way, which maximizes IoRT-based application productivity and efficiency [8].

The Internet of Robotic Things (IoRT) generates huge amounts of data from sensors, robots, and other de-

* Corresponding Author

vices. The statistics can be analyzed in real-time or stored for future assessment, providing valuable insights for improving the overall performance of the robot, predicting safety needs, and making data-driven decisions. Artificial intelligence (AI) approaches [9] can be utilized to examine and manipulate data, facilitating advanced functionalities such as machine learning, natural language processing, and computer vision. Incorporating robots onto the Internet increases security and privacy apprehension [10] as the robots and their data become linked to the online network. Securing robots' transmission, storage, and processing is essential to prevent unauthorized access, data breaches, and misuse. Data collection by robots, particularly in sensitive areas like healthcare and surveillance, may give rise to concerns over privacy. Security hazards refer to the risks associated with cyber threats and data breaches [11]. The IoRT [12] design faces several difficulties: security risks, privacy issues, reliability, robustness, connection, and compliance with rules. These issues reduce entire robotic performance in different applications. Hence, the IoRT design requires potential protocols, frameworks, and algorithms to minimize computation difficulties. Several researchers established established a method based on channel feedback to enhance physical layer security (PLS) in IoT systems [13]. However, they face privacy [14, 15] issues while developing the IoRT-based robotic systems. Then, the security issues are addressed with the help of intelligent learning techniques like Convolution Neural Networks (CNN) [16] and Deep Q Networks (DQN) [17].

Robots in IoRT systems need accurate and relevant information about certain situations to make informed decisions. Identifying, extracting, and using the right features for different contexts is difficult, which may lead to ineffective decision-making and a less efficient system. Data leaks, illegal access, and cyber-attacks are just a few security risks to which IoRT systems are susceptible. The criticality and difficulty of ensuring strong security measures to protect sensitive data and preserve system integrity cannot be overstated. Reliability and robustness in the face of unpredictable interruptions are key requirements for IoRT systems. Resolving hardware problems, communication failures, and environmental variations may impact the system's overall performance and reliability, an important part of ensuring robustness. IoRT systems must be able to incorporate new robotic applications and adapt to changing conditions without requiring costly reconfiguration. Such adaptability necessitates using adaptive algorithms and scalable structures, which may be challenging to develop and execute.

This study is motivated by the need to improve the performance of Internet of Robotic Things (IoRT) systems by using the combined advantages of Convolutional Neural Networks (CNNs) and Deep Q-Networks (DQNs). Our objective is to overcome the shortcomings of current methods by creating a unified system that can analyze intricate sensory information and make the best choices instantly, resulting in enhanced efficiency and flexibility of Internet of Robotic Things (IoRT) systems. The technical contribution includes efficient feature extraction and effective decision-making in IoRT systems, which are made possible by this study's innovative approach, which blends CNNs with DQNs. Numerous studies confirm that our methodology is more successful than current approaches regarding decision-making speed, task accuracy, and system efficiency.

The integrated CNN and DQN approach has several learning and activation functions that reduce the security difficulties in robotic applications. This study uses a camera as the sensor device that captures all the visual data in the surroundings. The recorded visual information is processed by convolution networks that minimize the computation difficulties while classifying the objects. The CNN extracts the hierarchical features from the visual data, which is inputted into the DQN approach. The DQN approach utilizes the reinforcement learning technique to help make effective decisions. Techniques like federated learning are employed to ensure the preservation of individual privacy. The hybrid architecture minimizes connectivity problems and maximizes robotic performance in different applications. In addition, it is utilized for continuous learning from user interactions, promoting trust, engaging the user, and minimizing trust-related issues. This integration enhances the performance of IoRT and incorporates adaptability, responsiveness, and ethical considerations. The proposed IoMT design novelty is leveraging the strengths of both methodologies: the powerful feature extraction capabilities of CNNs and the decision-making efficiency of DQNs. It enables more efficient processing and learning from high-dimensional sensory data typical in IoRT environments.

Then, the overall objective and novelty of the study are listed as follows.

(1) Optimize the IoRT system design by incorporating the CNN and DQN techniques to enhance robotic performance and efficiency.

(2) To improve the security measures by balancing the CNN and DQN to make the adaptive decision and mitigate the security threats in robotic performance.

(3) To establish an IoRT system to meet the robust, flexible, secure, and ethically acceptable requirements, capable of adjusting to changing backgrounds and user demands, and promote acceptance and confidence in implementing the IoRT.

Then, the overall paper is organized as follows: Section 2 discusses the various researcher's opinions regard-

ing the robotic performance in IoRT systems. Section 3 describes the working process of CNN and DQN approach to improve the IoRT robotic performance and the system's efficiency, which is evaluated in section 4. The conclusion is described in Section 5.

2 Related Works

Mahajan et al. (2023) [18] applied deep learning techniques in IoRT systems to create the robot motion detection system. The main intention of this study is to develop a reliable and robust motion detection process. In addition, the trustworthy framework is incorporated to manage the security of IoRT systems. The deep learning process uses multiple layers to explore inputs that identify the movement of robots. The system's effectiveness is evaluated using an experimental study in which the system ensures fast and accurate movement detection. However, the system faces difficulties and complexity while analyzing dynamic change environment-related robotic movements.

Liu et al. (2020) [19] recommended reinforcement learning and imitation learning processes to develop smart city robotic systems. This study uses the urban environment to identify changes in the surroundings. The deep learning process uses rewards for every state and action that helps to identify the robotic behaviour. The rewards predict every behaviour change that predicts the complexity of the urban environment. The effective utilization of reinforcement learning maximizes the robot's responsiveness and agility.

An AI-powered, real-time traffic monitoring system was developed by Kheder and Mohammed in 2023 [20]. The study aimed to develop a smarter, more adaptive monitoring system to enhance traffic management. To avoid traffic problems, the study constantly explores urban traffic congestion. The researchers used deep learning techniques and robotics enabled by the Internet of Things to create a system that can provide traffic patterns. The results show evidence of the suggested system's effectiveness and accuracy in real-time traffic monitoring and analysis.

The critical issue of detecting and controlling wildfires through developing a cyber-physical system is the subject of Battistoni et al. (2023) [21]. The system aims to recognize firefighting in wildfire scenarios. The information is collected from the scenarios processed by applying deep learning. The learning process uses several training patterns, which help to identify firefighting with limited resources. However, the system requires an adaptable and robust infrastructure to improve wildfire detection accuracy with a minimum error rate.

Vermesan et al. (2020) [22] explore the IoRT system connectivity and platform to maximize the robotic integration framework. The main intent of this study is to explore the various researchers' opinions, methodologies, and trends in IoRT applications. The research work provides learning technologies to enhance overall robotics productivity and collaboration. However, robotic systems face difficulties in managing compatibility during visual data analysis. Thamizhvani et al. (2021) [23] integrate various planning algorithms, control strategies, and artificial intelligence techniques to improve IoRT performance. During the analysis, learning techniques were utilized to understand the environmental conditions, which helped to maximize the decision-making ability in robotic applications.

Ramalingam et al. (2021) [24] developed AI integrated IoRT enabled framework to monitor the false ceiling environment. The research intention is to reduce the risk and false ceiling inspection prediction rate. During the analysis, Falcon robots were developed to monitor false ceiling activities. The robot-collected information is processed by a faster ResNet algorithm that predicts objects in the ceiling environment. The learning algorithm uses various image patterns to predict the changes in the ceiling. The system's efficiency is evaluated using different measures in which the system ensures a good confidence level and rodent prediction accuracy.

In their study, Vermesan et al. (2022) [25] investigate the Internet of Robotic Things (IoRT) converging actuating and hyperconnectivity using artificial intelligence techniques. This study uses the IoT heterogeneous processing to make effective communication. During the analysis, intelligent collaborative device robots are utilized to gather the information. The collected information is processed and maintained dynamically to improve the overall IoT integration in robotic applications. In addition, this study covers various architecture, technologies, and IoT concepts to improve the overall IoRT performance.

Based on the survey, there are several issues with existing models in attaining high system robustness, reliability and security enhancement. According to various researcher's studies, the Internet of Robotic Things (IoRT) is widely applied in various applications to improve their efficiency. During the analysis, the robots sense a lot of information from the sensors to collect and process the information. The gathered information helps understand the situation and environment, reducing computation difficulties while examining the complex scenario.

However, the study requires flexible, durable, and robust techniques to improve the overall robotic performance. Therefore, this study utilizes the combination of Convolution networks and deep Q networks to explore robotic activities and improve overall decision-making while analyzing data in IoT applications.

3 Performance Enhancement of the Internet of Robotic Things using Integrated Convolution Networks with Deep Q Networks

The main intent of this study is to create effective IoRT systems using convolution neural networks (CNN) with Deep Q Networks (DQN). During this process, security measures are enhanced by balancing the CNN and DQN to make effective decisions. Successful decisions help mitigate security threats to robotic performance. Then, the developed IoRT system should be computable with the environmental change by ensuring robustness, flexibility, and security. In addition, IoT integrated with robotic processes adapts to user demands, which helps to manage the acceptance and confidence in implementing IoRT.

3.1 Optimizing the IORT System Design using Integrated CNN and DQN Techniques

The main objective of this research was to optimize the IoRT system design using the integrated CNN and DON techniques. The optimized IoRT system can improve decision-making and maximize performance while analyzing real-time data. The convolution network has different parameters and objective functions that fine-tune the process, which helps to minimize the latency, computation load, and resource utilization. The convolution networks process the images, although they have noise images. The convolution network has convolution filters and kernel values that effectively help identify the objects from the visual. The convolution network has transfer learning, a weight-sharing mechanism, parameter setting, a pooling layer, and feature learning characteristics. These characteristics help to identify the objects and patterns from the visual object-related features. The extracted features are processed by the DQN approach, which uses reinforcement learning strategies to help balance the dynamic environment's decision-making process. The convolution network identifies every object changes and abnormal activity-related patterns. These patterns are processed using the DQN technique, which makes the security-related decision. The architecture of the IoRT system is explained in Fig. 1, which has several components such as visual data collection, hierarchical feature extraction using convolution networks, decision-making using DQN, optimization and feedback loop analysis and robotic component construction.

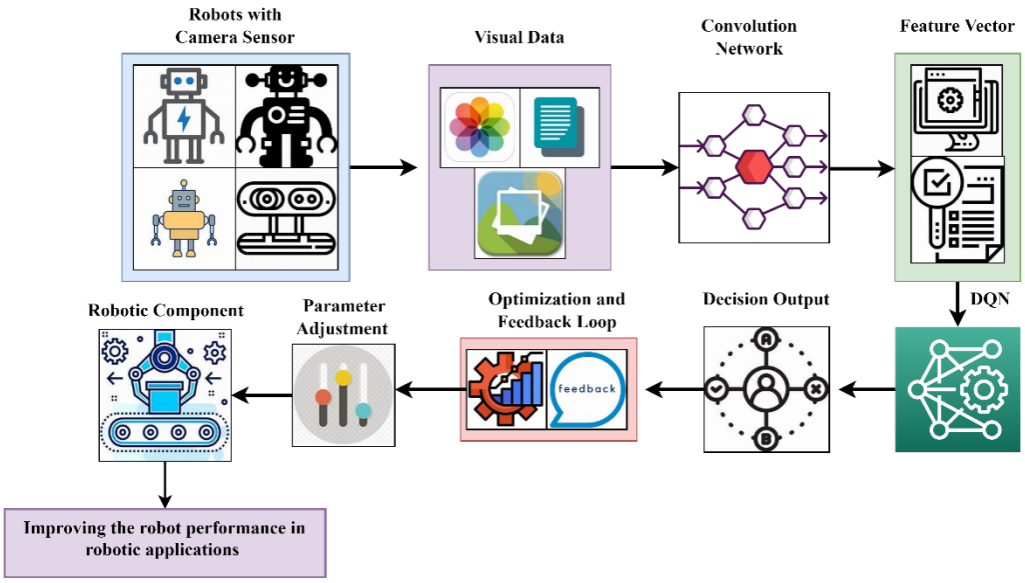

Fig. 1. Process of optimizing the IORT system design

According to Fig. 1, the CNN approach is utilized for image analysis, and DQN is used to make a suitable decision. The organized workflow of the IoRT commences with receiving visual information obtained from cameras, resulting in a continuous flow of images or video. The camera-based recorded scenario images or videos are stored in the database integrated with the IoT devices. The Convolutional Neural Network (CNN) is applied to the raw visual data to explore the features of the visual data. The convolution network explores every input and analyzes the complex hierarchical characteristics of the input information. The convolution network uses various components like the convolution layer, max-pooling, and a fully convoluted layer. These layers have the kernel or filter value that derives the image features like mean, standard deviation, contrast, and other features. The extracted features are fed into the Deep Q Networks (DQN) with the Q-learning algorithm, which helps make security-related decisions. The learning algorithm has reward values for every action and state. The learning process helps to decide on the features of the security threats and unauthorized activities in various environmental conditions. The adaptability of the IoRT systems is improved by applying the optimization and feedback loop. The optimization process uses the network's weight and bias values to compute the given input's output. The network parameters are updated according to the optimization functions and learning rate. The computed output value is compared with the training patterns, identifying the error value between the outputs. The feedback loop helps to maximize the flexibility and enhance the overall performance of the IoRT systems. After adjusting the network parameters, robotic components are created by fine-tuning the network performance. Then, the adjustments are performed according to the changes in the dynamic environment. The Internet of Things (IoT) embedded robotic sensor-based collected information is fed into the CNN for visual data processing. The robotics team has cameras continuously observing the environment; visual details are gathered frequently. The gathered information is processed by CNN components like convolution, pooling, and fully connected layers. The input processed by CNN is illustrated in Fig. 2.

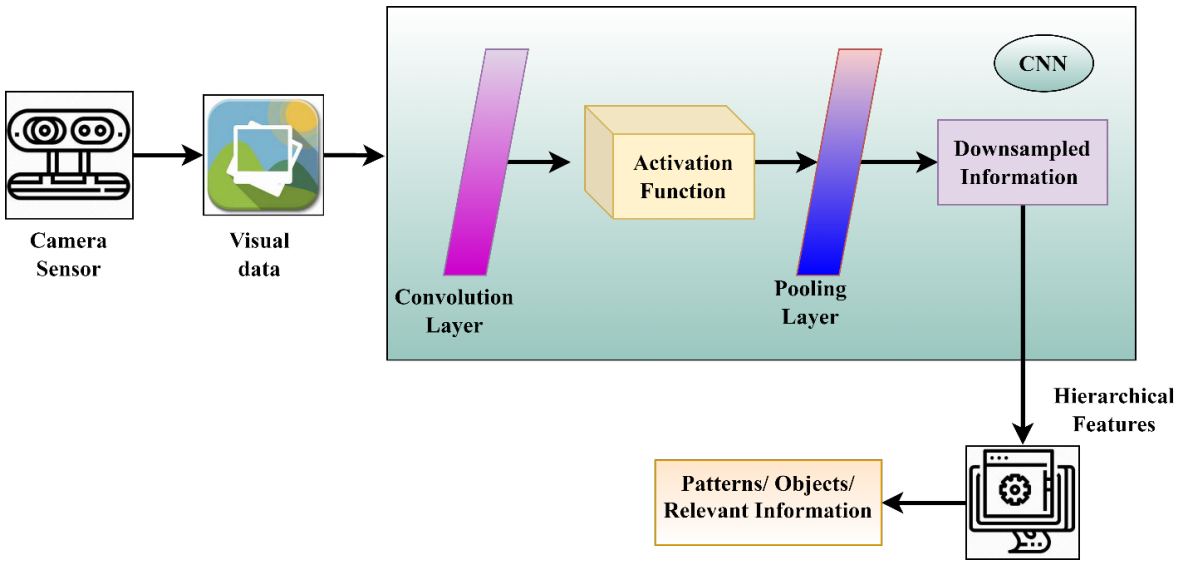

Fig. 2. Process of convolution neural networks

Fig. 2 represents the convolution neural network-based input processing for creating the effective IoRT system. Initially, the cameras embedded in the robotics gather the visual information. The collected visual data is fed into the convolution layer that extracts the hierarchical features. This process uses the activation function; here, the Rectified Linear Unit (ReLU) activation function is utilized as the non-linearity function that successfully extracts the features. Then, the pooling layer function is applied to downsample the information. This study uses the max-pooling function to generate the condensed representation of the features. The extracted features are fed into the decision-making process to improve the overall IoRT system design. The extraction of hierarchical features from visual input using a Convolutional Neural Network (CNN) encompasses several layers, such as convolutional layers, activation functions, and pooling layers. The standard equation for an individual layer in a Convolutional Neural Network (CNN) is defined in equation (1)

$$\theta = \delta(\mathbb{C}(\iota, \xi) + \beta) \quad (1)$$

In equation (1), convolution θ output is obtained by processing the input ι and filters ξ along with bias value β on the convolution process C using the activation function δ. The input (ι) correlates to the unprocessed visual information, typically an image or a feature map derived from the preceding layer. The convolution operation (C) involves applying filters (ξ) to the input. This process detects and represents spatial patterns present in the data. The mathematical representation involves calculating the dot product between the filter and a specific portion of the input δ(C(ι,ξ)+β). A bias (β) term is included in the convolution result to offset the output and enhance the model's adaptability. The activation function (δ) incorporates the Rectified Linear Unit (ReLU) as the non-linear activation function for the output. The output computation procedure described in equation (1) is continuously applied on the multiple CNN layers to extract the hierarchical features. Each layer is designed to derive intricate patterns from the visual inputs of different applications. The extracted high-level features are derived from the visual information, including image patterns, relevant information, and objects. The derived features are utilized as input because the features consist of various patterns and feature representations. The features are applied to the DQN to make a decision that helps to maximize the IoRT performance in the dynamic situation. The DQN has a set of learning rules, states and actions to process the inputs. Each state and action has connections that establish the link between input and output, enhancing the decision-making ability. The DQN has the agents in the reinforcement learning process that observe every scenario, improving the overall decision-making process. The agent gets feedback in every process, and rewards are obtained while the hierarchical features are processed. Then, the concept of DQN is illustrated in Fig. 3.

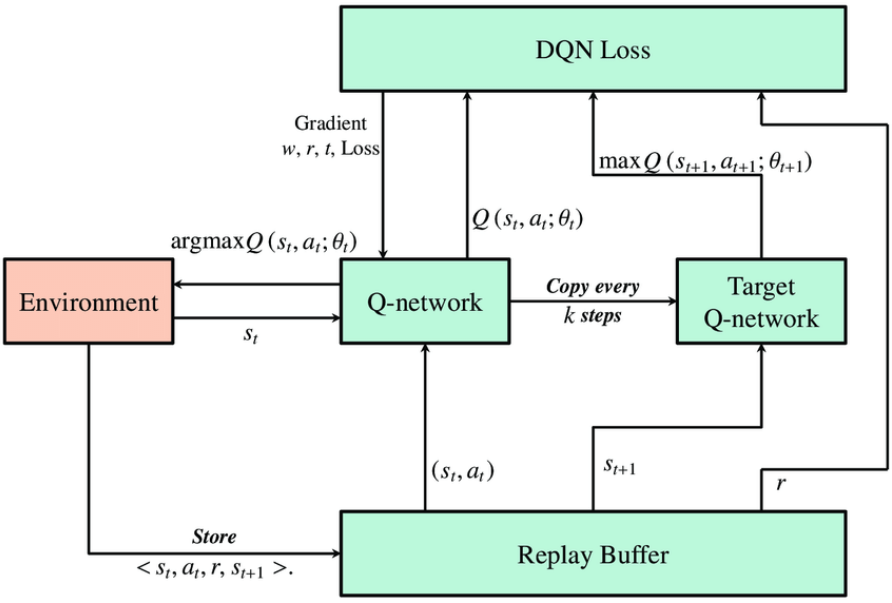

Fig. 3. Working process of DQN technique in decision-making

The Deep Q Network (DQN) has the Q function, denoted as Q(s,a); s represents the system's state, while a represents an action. The Q-value represents the projected total reward obtained by selecting action an state s. The DQN utilizes a neural network to approximate its Q-function. The neural network receives the state as an input and produces Q-values for every feasible action. Then, the Q function is defined as Q(s,a)≈Q_θ (s,a); here, Q_θ (s,a) is an approximation of Q(s,a) using the parameters represented by θ in the neural network. The computed Q-values are collated with the expected and actual Q-values in the learning environment to minimize the deviation while making decisions. The learning updating process is defined in equation (2).

$$Q(s,a) \leftarrow Q(s,a) + \alpha(R + \gamma max_{a'} Q(s',a') - Q(s,a)) \quad (2)$$

In equation (2), the Q value for the present state-action pair is denoted as Q(s, a), the immediate reward got after action a in state s is represented as R, and the discount factor (future reward) is denoted as γ, next state action pair on Q value is defined as Q(s^',a^') and the learning rate is α. At first, the IoRT system acquires visual input, such as images from a camera that is processed using CNN. The Convolutional Neural Network (CNN) has a unique ability to detect hierarchical features in visual data, creating an effective feature vector that encapsulates the most significant attributes of the input. After classifying the inputs and hierarchical features, the output is compared with the training features. The comparison process reduces the overall misclassification and false decision rate. This study uses the gradient boosting algorithm to optimize the network performance. The boosting procedure reduces weak feature involvement and improves overall recognition accuracy and decision-making efficiency. The boosting process uses the learning rate, architecture parameters, layer size and dropout rates to fine-tune the CNN performance. The errors are corrected by reducing the weak feature involvement by predicting the feature set's ensembles F(x). F(x) is continuously updated for every iteration to minimize the error rate.

$$F(x) = F_{t-1}(x) + \eta . h_t(x) \tag{3}$$

In equation (3), F(x) is represented as the predicted ensembles in t-iteration, the learning rate is denoted as η, and the new weak learner is represented as h_t (x). After identifying the ensemble features in the feature, the learning rate is updated continuously to minimize the output deviations. The learning rate updating process is defined using equation (4)

$$\alpha_t = \alpha_{t-1} - \eta . \frac{\partial L(\alpha_{t-1})}{\partial \alpha_{t-1}} \tag{4}$$

In equation (4), the learning rate is represented as η, which helps to maximize the CNN performance. The learning rate is fine-tuned with the help of gradient boosting, which minimizes the loss function. After fine-tuning the parameters, feedback is received continuously. The received feedback is utilized to construct the robotic components, which can process the information in various scenarios.

3.2 Enhancing the Security Measures in IoRT using Integrated CNN and DQN Technique

Integrating the two strategies of Convolutional Neural Network (CNN) and Deep Q Network (DQN) would be vital for IoRT security enhancement. This extensive plan aims to quickly identify and fix any security glitches that may arise while ensuring that the IoRT system has a strong and flexible security architecture. Deep Networks (DQN) and Convolutional Neural Networks (CNNs) need careful examination while developing a well-rounded security approach. CNN's power comes from its ability to scan images to identify patterns, allowing it to examine visual data deeply for any potential problems. Conversely, DQN does adaptive decision-making with great efficiency. By balancing these two approaches, threat detection can easily be integrated with smart decision-making. If we want to achieve the highest degree of security possible, we may need to adjust factors such as their weights and designs regarding CNN's strength and DQN's strengths.

To enhance the effectiveness of security measures, researchers have developed a novel approach that combines Convolutional Neural Networks (CNN) and Deep Q-Networks (DQN). This adaptive decision-making technique allows the Internet of Robotic Things (IoRT) system to respond promptly to evolving threats by efficiently addressing unexpected challenges, swiftly adjusting security policies, and optimizing responses following dynamic threat landscapes. Integrating CNN and DQN methods establishes an organized and adaptable strategy for bolstering IoRT security while ensuring privacy considerations. The initial stage of this integration involves leveraging CNN's pattern recognition capabilities to rapidly identify potential threats through visual inputs obtained from sensors or cameras. A harmonious equilibrium is achieved between the two approaches by delegating threat identification tasks to CNN and empowering DQN to adaptively make judgments based on these identified threats. Training DQN entails establishing correlations between actions taken by IoRT systems and their corresponding states to enable real-time decision-making optimization as security situations evolve. By analyzing environmental information and the efficacy of previous safety precautions, DQN's reinforcement learning algorithms enable adaptive responses. The integrated system is optimized by iterative parameter refinement employing an optimization loop, which continuously adjusts hyperparameters. Feedback systems informed by real-time danger and performance feedback enhance the system's adaptability. The control mechanisms of robot-

ic components integrate seamlessly into the final decision output, ensuring that security judgments are translated into productive activities. Constant vigilance, evaluation, and collaboration with security experts strengthen the security architecture as an entire system. This guarantees that the framework can respond to new security threats and satisfy the growing demands of the IoRT ecosystem.

3.3 Establishing a Robust IoRT System for Promoting Acceptance and Confidence

This section analyzes the robustness of IoRT systems, which helps determine how effectively the integrated CNN and DQN-based crated system adapts to the environment according to user requirements. The IoRT system's robustness is evaluated using different aspects to determine the system's uncertainties and fluctuations in various scenarios. In addition, the robustness factor measures how effectively the created robots improve the system performance in various operational strategies. Here, the captured camera visual data is processed using the convolution network to process the noise image with minimum computation complexity. The convolution network has max-pooling and convolution layers that minimize the feature map and downsample the feature. Effectively utilizing these layer functions ensures design flexibility and can adapt the system to changing environments. Then, the IoRT systems are developed with predefined configurations and setups that ensure the system's adaptability and adjust to the dynamic environment over time. The convolution layer derives the feature maps and hierarchical features that are compared with the training patterns, which helps predict the environment's vulnerable external actions. The extracted features are processed by deep Q networks that predict the decision according to the features, which ensures the system's robustness and security in the dynamic environment.

The next important factor in system robustness is simultaneously accepting and developing confidence between the users and participants in the IoRT system. The IoRT system should prioritize the user requirements that ensure user acceptance and user-friendly interfaces, which ensures that the robotic system can adapt to the IoT technologies and relevant integrations. Then, the IoRT system confidence level is improved by checking the system's dependability, security measures, and ethical principles. Then, the IoRT system should follow certain safety protocols that establish clear communication between robotics and the user, which helps to maximize the overall performance of the IoRT systems. The extracted features are processed by convolution and Q-learning techniques, encouraging practical usability and trust between the users and the robots. The reason behind this is to make the IoRT system reliable and confident and then involve CNN and DQN methodology. In this way, it will be ensured that the system is robust, flexible, and ethical. This is because decision-making adjusts based on the hierarchical features by effectively applying convolution neural function and reinforcement learning process.

On the other hand, the CNN approach collects visual data and investigates visual features that recognize objects and patterns. These patterns provide an understanding of weather conditions, hence ensuring robustness. The DQN enables flexibility in decision-making processes by learning knowledge and adapting to changing environments and user requirements. Intricate security protocols are integrated into the technology to safeguard from external intrusions while observing ethical norms. The combination of CNN and DQN enhances the security of IoRT by giving superior threat detection capabilities and adaptable responses, thereby making the system operate ethically.

4 Results and Discussions

This section discusses the excellence of the combined CNN and DQN-based created IoRT system efficiency in various robotic applications. The robotics are integrated with the IoT techniques to monitor the surrounding activities such as object detection, surveillance systems, anomaly identification, etc. These application requirements are dynamically changed, which affects the robotic decision-making capability and object detection efficiency. Therefore, the integrated CNN and DQN approach is introduced in this study to maximize the object detection and decision-making process. The IoT devices in robotics continuously record surrounding information in terms of data, video, and images. This study uses camera sensors to record the visual data stored in the IoT-integrated database. The convolution network processes the images using various kernel values that derive the hierarchical features. The extracted features are downsampled with the help of the max pooling layer, reducing the computation difficulties. The derived features are processed by the DQN approach, which manages decision-making efficiency with the help of the Q-learning mechanism. In addition, reinforcement learning uses reward values for every action and state, reducing decision-making difficulties. Then, the system efficiency is determined using

various factors such as perception identification improvements, system robustness, decision-making, and security evaluation. The perception analysis covers object detection rate, precision, and recall value for various visual scenarios. The adaptive decision-making metric is analyzed using the learning rate, decision accuracy, and exploration-exploitation factors. The perception and decision-making factors help to understand how effectively the IoRT system monitors the dynamic changes in the environment. The efficiency determines how effectively the IoRT system recognizes the objects, security threats and decisions concerning user demands. Combining CNN with DQN allows for much faster decision-making, a major benefit. Delays are common in traditional IoRT systems because processing sensory input and making judgments requires a lot of CPU power. The proposed method uses CNN's parallel processing capabilities to extract beneficial features from sensory inputs quickly. These attributes are inputted into the DQN, effectively ascertaining the best action. Efficient use of computing resources and energy consumption are both components of a system's efficiency. By distributing workloads between the CNN and DQN, our integrated strategy minimizes the computational complexity, allowing each component to function within its strengths.

Then, the overall efficiency of the system is evaluated as follows.

4.1 Perception Enhancement Accuracy Analysis (PEAA)

The PEAA metric is analyzed using object recognition, recall, and precision rates. The object identification rate computes from the convolution network performance. The convolution network uses different functions that identify the objects, patterns, and relevant information from the total number of objects. Then, the recall rate, named the true positive rate, computes how effectively the convolution network predicts the correct objects from the entire number of existing relevant objects in the visual data. Finally, the precision metric computes the degree of accuracy from the correctly detected significant objects. According to these factors, the PEAA value is computed by taking the average value of the total number of detected objects. The sample PEAA value is illustrated in Table 1.

Table 1. PEAA analysis

Visual area scenario	Recognized objects	Relevant objects	Identified relevant objects
Sample scenario 1	93	100	92
Sample scenario 2	90	94	89
Sample scenario 3	95	100	93
Average	$\left(\frac{Totally\ \ Correctly\ \ identified}{Total\ \ Objects}\right)$	Total relevant objects across all scenarios	Total correctly Identified relevant objects
Average results	92.66%	98%	91.3%

Table 1 shows that the integrated CNN and DQN in the IoRT system are evaluated for perception enhancement metrics by considering the object recognition rate, precision, and recall rate. The system's efficiency is determined using three visual scenarios in which visual information is recorded with the help of the camera. The visualized details are classified using convolution networks, and the method recognizes the objects with a maximum recognition rate. Integrating Convolutional Neural Network and Deep-Q-Network for the Performance Enhancement of Internet of Robotic Things between $\left(\frac{Totally\ \ Correctly\ \ identified}{Total\ \ Objects}\right)$. The total relevant objects across all scenarios are computed to estimate the relevant object detection rate, and the total correctly identified relevant objects are computed to predict the precision rate. Then, the graphical analysis of the PEAA is shown in Fig. 4.

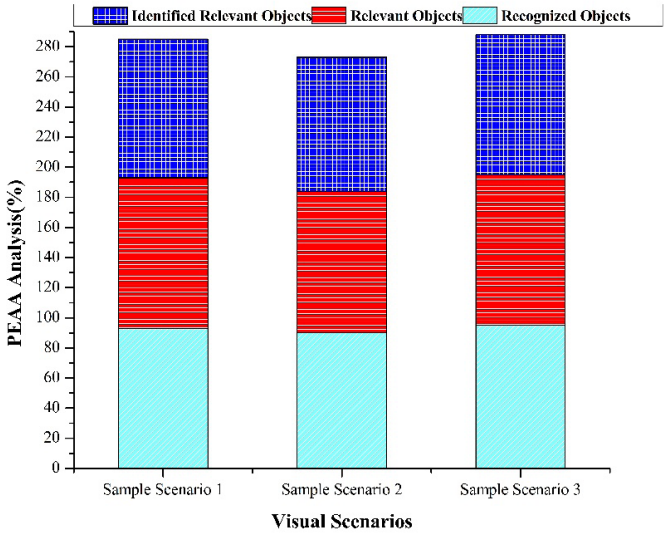

Fig. 4 Graphical analysis of PEAA

The analysis (Fig. 4) shows that the integrated CNN and DQN approach attains the 92% recall and precision value in scenario 1. From the computed value, the average results are estimated in which the CNN and DQN approach attains 92.66% accuracy while discovering the objects from the visual data. Thus, the high recognition rate, precision, and recall value indicate that the system ensures a high PEAA value in IoRT scenarios. Thus, the system effectively identifies the objects even though the environment dynamically changes their condition.

4.2 Adaptive Decision-Making Efficiency Analysis (ADMEA)

The metric Adaptive Decision-Making Efficiency Analysis (ADMEA) measures the excellence of the DQN approach in the IoRT systems. The ADMEA measure considered different metrics such as decision accuracy, learning rate, and exploration-exploitations. The decision accuracy is computed to measure how exactly the DQN decides while the unwanted activities in IoRT. The decision helps to manage the system's security and privacy. During this process, a learning rate is applied that computes how effectively DQN regulates the decision according to the dynamic changes of the surrounding environment. The maximum learning rate indicates that the designed IoRT system highly adapts to environmental changes. Another factor is exploration-exploitations, which quantify the system according to the previously gained knowledge. This factor analyzes the ideal equilibrium between the existing knowledge and new possibilities in the IoRT systems. Therefore, the AEMEA analysis explores the IoRT system's adaptability to unexpected changes. Then, the sample value of ADMEA is shown in Table 2.

Table 2. ADMEA analysis

Scenario	Decision accuracy	Learning rate	Exploratin-exploitation
Decision scenario 1	98	High	Balanced
Decision scenario 2	94	Medium	High
Decision scenario 3	96	Low	High
Average	$\left(\frac{Totally\ \ Correctly\ \ decided}{Total\ \ decision}\right)$	Total learning rate across all scenarios	Balanced exploration and Exploitation across all the scenarios.
Average results	96%	Medium-High	Balanced

Table 2 evaluates the IoRT system's Adaptive Decision-Making analysis considering the decision accuracy, learning rate, and exploration-exploitation. Every scenario tests the IoRT system's accuracy, adaptability based on experience, and ability to balance innovative and learned decision-making strategies using the Deep Q Network. From the analysis, the scenario DQN attains 98% accuracy because it uses reinforcement learning techniques. The learning techniques have a reward value for every action and state. During the learning process, the network uses different learning rates, and a high learning rate indicates that the system effectively decides the derived hierarchical features. In addition, the integrated CNN and DQN techniques balance the exploration-exploitation process while exploring the visual features. From Table 2, the ADMEA achieves 96% accuracy with a medium-high learning rate and balances the features during the analysis. The balancing process and exploiting depicted the system intelligence while deciding the IoRT.

4.3 System Robustness Analysis (SRA)

The next metric is the system robustness analysis (SRA) of the IoRT system. The SRA efficiency is measured in terms of adaptability index and system reliability. The reliability measure indicates that the created IoRT system should be able to work under various criteria in the given scenario. The adaptability index analyses how the CNN-DQN-based created IoRT system adapts to changes according to user demands and environmental conditions. The adaptability measure understands the observance of the user demands and changes in the dynamic scenario. Then, the high SRA value indicates that the system ensures user-friendliness and resilience in the IoRT system. Then, the sample value for SRA in different scenarios is depicted in Table 3.

Table 3. SRA analysis

Scenario	System reliability	Adaptability index
Scenario 1	High	High
Scenario 2	High-Medium	Medium
Scenario 3	High	High
Average	$\left(\frac{Totally\ \ reliable\ \ sceneario}{Total\ \ sceneario}\right)$	Total adaptability index across all scenarios
Average Results	High	High

Table 3: Table 3 illustrates the SRA analysis of designed IoRT systems. Here, the analysis is carried out with the help of system reliability and adaptability index metrics. The IoRT system efficiency is determined in various scenarios. If the system attains high system reliability and high adaptability index value, then the system attains high SRA values. The results clearly state that the CNN design with a DQN-based IoRT system ensures robustness in various applications.

4.4 Security Enhancement Analysis (SEA)

The other metric is the Security Enhancement Analysis (SEA) of designed IoRT systems. The SEA metric regarding threat detection accuracy, security decision precision, and ethical score is evaluated. How effectively does CNN classify the surrounding visual data and predict the accuracy of threat detection? The high-value detection accuracy indicates that extracted hierarchical features successfully identify irrelevant activities and unauthorized actions. The extracted features are processed by DQN, which decides with high accuracy. The high decision accuracy indicates that the system ensures maximum reliability and security. The ethical operation score is computed based on the threat detection accuracy and the decision precision value. The maximum ethical score indicates that the IoRT system successfully considers ethical considerations and protects the data from security threats. Combining three metrics ensures that the designed IoRT system meets the security standards. In addition, the system can manage the safety and integrity of the IoRT system. The sample SEA value is illustrated in Table 4.

Table 4. SEA analysis

Scenario	Threat detection Accuracy	Security decision precision	Ethical operation score
Scenario 1	High	High	Very high
Scenario 2	High-Medium	Medium	high
Scenario 3	High	High	Very high
Average	$\left(\frac{Totally\ \ high\ \ accuracy\ \ sceneario}{Total\ \ sceneario}\right)$	$\left(\frac{Totally\ \ high\ \ precision\ \ sceneario}{Total\ \ sceneario}\right)$	$\left(\frac{Totally\ \ very\ \ high\ \ ethical\ \ score}{Total\ \ sceneario}\right)$
Average Results	High	High	High

Table 4 above depicts the SEA analysis of various scenario analyses of IoRT systems. The table shows the scenario has high threat detection accuracy, security prediction, and ethical operation score. These score values are computed for every scenario where the high value indicates that the system satisfies the security and robustness while observing the surrounding information. The average results row offers a comprehensive perspective across several circumstances, indicating the IoRT system's capacity to enhance security. As usual, these values are hypothetical and can be substituted with actual data obtained through testing and evaluation. According to the discussion, these scenarios aim to replicate various conditions, difficulties, or assignments that the IoRT system may face in practical situations. Every scenario evaluates several system performance facets, including perception, decision-making, security, resilience, and ethical conduct. Scenarios like public park smart surveillance are one of the scenarios. The metrics discussed in scenario one and the related objectives and descriptions are illustrated in Table 5.

Table 5. Scenario 1 discussions

Scenario 1: Public park smart surveillance		
Metrics	Objective	Description
PEAA	Analyzing and recognizing the objects in the park visual information	A camera placed in the part intends to identify and recognize objects like suspicious items, vehicles, and people.
ADMEA	Decisions are taken according to the park's visual information	Identifies dynamic situations like security threats in crowded areas and alerts the system for security concerns.
SRA	System reliability and adaptability analysis according to park condition	The system can operate in different weather conditions, like rainy and sunny.
SEA	Identify and respond to the security threats	It intends to predict suspicious activities in the park.

Likewise, human-robot collaboration in the warehouse and emergency response in urban regions is considered in scenarios 2 and 3 for evaluating the performance of the IoRT in real-time applications. Thus, effectively integrating the CNN and DQN techniques improves the overall robotic performance by identifying the hierarchical features from the visual inputs. This process attains high security, robustness, flexibility, and adaptability while analyzing the visual information.

5 Conclusion

Thus, the paper analyzes the various scenarios for improving the IoRT system performance in real-time applications. The visual data is collected with the help of a camera, which is processed by convolution networks that extract the high-level features. The convolution network applied the filter and max-pooling layers on visual data to extract the features. The derived features are processed by the DQN approach, which has a reinforcement learning process that decides the status of the features. The learning procedure has a reward value for every action and state that reduces the security threats. The combination of CNN and DQN helps to ensure the system's robustness and security and enhances the overall operational efficiency. The extracted visual features are utilized to recognize the objects in their surroundings with minimum computation complexity. During the process, convolution network parameters are fine-tuned frequently according to the learning patterns. The derived pattern helps to make adaptive decisions by managing the system's robustness, flexibility, and reliability. The discussed

system efficiency is evaluated in various scenarios in which the system ensures maximum security and robustness. However, this study has a limitation in that the system requires optimized techniques to reduce the computation difficulties while processing large volumes of real-time applications.

6 Acknowledgement

This work is supported by the 14th Five-Year Plan Project of Guangxi Educational Science "Research on the Classification Cultivation and Assessment Evaluation System for Professional Teachers in Vocational Colleges from the Perspective of Innovation and Entrepreneurship" (2022ZJY2788) and 2022 Liuzhou Railway Vocational and Technical College Science and Technology Innovation Team (2022-KJCX003).

References

[1] S. Vojić, Internet of robotic things (IoRT) applications, International Scientific Journal "Industry4.0" 4(2020) 156-159.
[2] S. Hong,Y. Hwang, Design and implementation for iort based remote control robot using block-based programming, Issues in Information Systems 21(4)(2020) 317-330.
[3] A. Koohang, C.S. Sargent, J.H. Nord, J. Paliszkiewicz, Internet of Things (IoT): From awareness to continued use, International Journal of Information Management 62(2022) 102442.
[4] L. Romeo, A. Petitti, R. Marani, A. Milella, Internet of robotic things in smart domains: Applications and challenges, Sensors 20(12)(2020) 3355.
[5] J. Kaur, S. Ganguli, S.L. Tripathi, The Roles of Artificial Intelligence, Machine Learning, and IoT in Robotic Applications, in: Internet of Things, 1st ed., CRC Press, 2022 (47-60).
[6] T. Gueye, Y. Wang, R.T. Mushtaq, M. Rehman, A. Ahmed, H. Ali, State of the art review on automatic sorting system for industrial robots using Internet of Robotic Things. <https://www.researchsquare.com/article/rs-2329674/v1>, 2022 (accessed 23.04.2024).
[7] R. Goel, P. Gupta, Robotics and Industry 4.0, in: A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development, Springer, Cham, 2020 (157-169).
[8] M. Javaid, A. Haleem, R.P. Singh, R. Suman, Substantial capabilities of robotics in enhancing industry 4.0 implementation, Cognitive Robotics 1(2021) 58-75.
[9] J. Zhang, D. Tao, Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things, IEEE Internet of Things Journal 8(10)(2021) 7789-7817.
[10] J.P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations, International Journal of Information Security 21(1)(2022) 115-158.
[11] L. Cheng, K.R. Varshney, H. Liu, Socially responsible ai algorithms: Issues, purposes, and challenges, Journal of Artificial Intelligence Research 71(2021) 1137-1181.
[12] A. Kumar, S. Sharma, A. Singh, A. Alwadain, B.J. Choi, J. Manual-Brenosa, A. Ortega-Mansilla, N. Goyal, Revolutionary strategies analysis and proposed system for future infrastructure in Internet of Things, Sustainability 14(1)(2022) 71.
[13] K.O. Chee, M. Ge, G. Bai, D.D. Kim, IoTSecSim: A framework for modelling and simulation of security in Internet of things, Computers & Security 136(2024) 103534.
[14] C. Karri, O. Cheikhrouhou, A. Harbaoui, A. Zaguia, H. Hamam, Privacy preserving face recognition in cloud robotics: a comparative study, Applied sciences 11(14)(2021) 6522.
[15] W. Xian, K. Yu, F. Han, L. Fang, D. He, Q.L. Han, Advanced Manufacturing in Industry 5.0: A Survey of Key Enabling Technologies and Future Trends, IEEE Transactions on Industrial Informatics 20(2)(2024) 1055-1068.
[16] M.D. Choudhry, B.A. Devi, M. Sundarrajan, Novel Optimized Framework for Video Processing in IoRT Driven Hospitals, Intelligent Automation & Soft Computing 34(1)(2022) 267-278.
[17] S. Shen, L. Xie, Y. Zhang, G. Wu, H. Zhang, S. Yu, Joint Differential Game and Double Deep Q–networks for Suppressing Malware Spread in Industrial Internet of Things, IEEE Transactions on Information Forensics and Security 18(2023) 5302-5315.
[18] H.B. Mahajan, N. Uke, P. Pise, M. Shahade, V.G. Dixit, S. Bhavsar, S.D. Deshpande, Automatic robot Manoeuvres detection using computer vision and deep learning techniques: a perspective of Internet of robotics things (IoRT), Multimedia Tools and Applications 82(15)(2023) 23251-23276.
[19] Y. Liu, W. Zhang, S. Pan, Y. Li, Y. Chen, Analyzing the robotic behavior in a smart city with deep enforcement and imitation learning using IoRT, Computer Communications 150(2020) 346-356.
[20] M.Q. Kheder, A.A. Mohammed, Real-time traffic monitoring system using IoT-aided robotics and deep learning techniques, Kuwait Journal of Science 51(1)(2024) 100153.

[21] P. Battistoni, A.A. Cantone, G. Martino, V. Passamano, M. Romano, M. Sebillo, G. Vitiello, A cyber-physical system for wildfire detection and firefighting, Future Internet 15(7)(2023) 237.
[22] O. Vermesan, R. Bahr, M. Ottella, M. Serrano, T. Karlsen, T. Wahlstrøm, H.E. Sand, M. Ashwathnarayan, M.T. Gamba, Internet of robotic things intelligent connectivity and platforms, Frontiers in Robotics and AI 7(2020) 104.
[23] T. R. Thamizhvani, R.J. Hemalatha, R. Chandrasekaran, A.J.A. Dhivya, AI, Planning and Control Algorithms for IoRT Systems, in: Human Communication Technology: Internet of Robotic Things and Ubiquitous Computing, Scrivener Publishing LLC, 2021 (Chapter 7).
[24] B. Ramalingam, T. Tun, R.E. Mohan, B.F. Gómez, R. Cheng, S. Balakrishnan, M.M. Rayaguru, A.A Hayat, Ai enabled IoRt framework for rodent activity monitoring in a false ceiling environment, Sensors 21(16)(2021) 5326.
[25] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, C. Gallicchio, A. Micheli, M. Dragone, A. Saffiotti, P. Simoens, F. Cavallo, R. Bahr, Internet of robotic things–converging sensing/actuating, hyperconnectivity, artificial intelligence and IoT platforms, in: Cognitive Hyperconnected Digital Transformation, 1st ed., River Publishers, New York, 2021 (97-155).