Enhancing QoS in 5G IoT with CNN and Blockchain Security vs. Deep Reinforcement Learning

Jeya Darshini and V. Nagaraju
Saveetha University, Chennai, Tamil Nadu, 602105, India

Keywords: 5G-Enabled Internet of Things, Novel Convolutional Neural Network, Deep Reinforcement, Blockchain Framework, Intrusion Detection, Network Infrastructure.

Abstract: In this research, the efficiency of both Novel Convolutional Neural Network (CNN) and Deep Reinforcement Learning (DRL) was assessed in enhancing the Quality of Service (QoS) for 5G-enabled intelligent Internet of Things (IoT) systems. Using data from the Kaggle repository with a sample size of 5840, an 80% G power and a 95% confidence interval were established. Two groups of 20 iterations each were divided, with Novel Convolutional Neural Networks making up the first group, and Deep Reinforcement Learning constituting the second. The results revealed that the accuracy of Deep Reinforcement Learning stood at 70.70%, whereas the CNN yielded an 84.64% accuracy rate. A marked difference of 0.405 between the two groups was observed, indicating non-significance. Therefore, it's evident that CNNs offer superior QoS accuracy over Deep Reinforcement Learning.

1 INTRODUCTION

The advancement of intelligently-enabled Internet of Things (IoT), powered by 5G technology, has transformed our everyday experiences. 5G technology facilitates faster, more dependable communication networks, laying the foundation for the evolution of smart wearables, healthcare systems, and other IoT services. It offers low latency, great scalability (Qi and Liu 2018), and a refined network infrastructure that ensures efficient data processing and communication. The advent of 5G also allows real-time data transmission, enhancing communication and user experience. This innovation supports the connection of myriad devices to a singular network, ensuring smooth communication. A 5G-ready IoT application (Rathore et al. 2021) promises to optimise user satisfaction, service quality, and network experience by connecting a vast number of devices. To guarantee the secure transmission of data without depending on a central authority, blockchain technology has been recommended. Utilising a distributed ledger system, blockchain offers a P2P transaction platform, ensuring data is safely, ncryptedly, and decentralisedly recorded, verified, and exchanged (R. Pavaiyarkarasi et al. 2022). This technology promises heightened security and privacy for next-generation network communication infrastructures (Deena, S. R et al 2022). Blockchain's decentralisation, security, and anonymity (Mahapatra, S et al. 2016) have the potential to be revolutionary for 5G-enabled IoT networks. To evaluate the efficiency of these innovations, it's imperative to employ Quality of Service (QoS) metrics (Pradhan et al. 2021), encompassing factors like accuracy, latency, and security. Our methods incorporate QoS factors, ensuring their effectiveness in 5G-enabled IoT applications (Pradhan et al. 2021; Verhelst and Moons 2017). They guarantee the successful deployment of real-time applications by providing a secure and adaptable environment for 5G IoT devices.

Recent research has strived to enhance firewall protection for IoT devices. As per Google Scholar, over 15,320 publications cover this area, and IEEE Xplore has 4,680 articles (Rathore et al. 2021). Incorporating a blockchain security framework with deep learning algorithms has been proposed for heightened privacy and accuracy. Some studies (Rathore et al. 2021; Anand and Khemchandani 2020) have highlighted security and privacy concerns within the fog computing system layers and suggested solutions involving cloud and edge planes. Another research (Sahu et al. 2021) focused on malicious attacks in the security layer, offering a blockchain framework to detect such attacks on 5G IoT devices using deep learning. These researchers emphasise the pressing need for robust security measures due to the

Darshini, J. and Nagaraju, V.
Enhancing QoS in 5G IoT with CNN and Blockchain Security vs. Deep Reinforcement Learning.
DOI: 10.5220/0012558800003739
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 58-63
ISBN: 978-989-758-661-3

inherent vulnerabilities of IoT devices. The collective application of blockchain technology and deep learning algorithms can significantly bolster IoT security.

Existing research indicates that combining Deep Learning algorithms with Blockchain firewall improves accuracy in 5G-enabled IoT devices. However, there's a noticeable gap in identifying threats. The Novel Convolutional Neural Network has been identified as a potent solution to counteract such threats. Moreover, there's an urgent need to investigate how the proposed strategies can address prevailing challenges in IoT systems, including security, scalability, and performance.

2 MATERIALS AND METHODS

At the Machine Learning Lab in the Saveetha School of Engineering, part of the Saveetha Institute of Medical and Technical Sciences, a comprehensive study was conducted. To enhance accuracy, each group underwent a series of 10 iterations. The dataset for this study was sourced from the Kaggle website. Python served as the primary programming language for all experimental procedures. The samples were methodically divided, with 80% designated for training purposes and the remaining 20% allocated for testing. Every group comprised 24 samples. A significance level of 0.05% and a confidence interval of 95% were set, with G-Power set at 80%.

The mean and standard deviation for the sample size were determined based on data collated from multiple websites (Riaz et al. 2022).

2.1 Novel Convolutional Neural Network

The Convolutional Neural Network (CNN) is a flexible neural network utilised for pattern recognition and image processing. It establishes a structured flow for training parameters through its input, convolution, pooling, and output layers. In the convolution layer, an input image undergoes filtering to derive feature maps essential for the convolution process. Subsequently, the pooling layer down-samples these feature maps using an activation function, scalar weighting, and bias. One significant advantage of a CNN is the parallel nature of its learning, which simplifies implementation. The computations and operations within a CNN's layers can be articulated by equations (1), (2), (3), and (4) (Tanwar 2021).

$$O_{x,y}^{(l,k)} = tanh\,(\sum_{t=0}^{f-1} \blacksquare \sum_{r=0}^{Kh} \blacksquare \sum_{c=0}^{Kw} \blacksquare (r,c)_{(r,c)}^{(k,t)}(x + r, x + c)_{(x+r,x+c)}^{(l-1,t)} + Bias^{(i,k)}, \tag{1}$$

Where $O_{x,y}^{(l,k)}$ is the output at layer L, feature pattern K, row x, column y of the convolutional core which is denoted by f.

Now, row x and y are expressed as:

$$O_{x,y}^{(l,k)} = tanh(W^{(k)} \sum_{r=0}^{Sh} \blacksquare \sum_{c=0}^{Sw} \blacksquare (x * Sh + r, y * Sw + c)_{(x*Sh+r,y*Sw+c)}^{(l-1,t)} + Bias^{(i,k)}) \tag{2}$$

The output is as follows in the hidden layer:

$$O_{(l,j)} = tanh(\sum_{k=0}^{s-1} \blacksquare \sum_{x=0}^{Sh} \blacksquare \sum_{y=0}^{Sw} \blacksquare (x,y)_{(x,y)}^{(j,k)} + Bias^{(i,j)}) \tag{3}$$

2.2 Algorithm

1. INPUT: Intrusion attacks in 5G-enabled IoT devices
2. OUTPUT: Accuracy of intruding attacks
3. Step 1: Collect network traffic data in a 5G-enabled IoT environment.
4. Step 2: Pre-process the data to remove any noise and outliers.
5. Step 3: Extract features from the data using the Novel Convolutional Neural Network (CNN) algorithms.
6. Step 4: Train the CNN model on the extracted features.
7. Step 5: Use the trained model to detect any anomalies in the network traffic.
8. Step 6: If any anomalies are detected, further classify them as malicious or benign using deep learning algorithms.
9. Step 7: Generate an alert for any malicious activities detected in the network.
10. Step 8: Take the necessary action to mitigate the attack and prevent further damage.

2.3 Deep Reinforcement Learning

Deep Reinforcement Learning (DRL) was used (Kim) in order to develop a caching technique for the 5G and subsequent mobile networks. The findings of their numerical data suggested that the devised DRL caching strategy was efficient at optimising caching resources. Moreover, this strategy was successful in decreasing the average energy consumption of edge computing devices for heterogeneous 5G mobile network technology. The Deep Reinforcement Learning model was trained offline in a central server with one simulated digital twin of an actual network environment. Results showed that the system proposed decreased the normalised energy usage more proficiently than current approaches while necessitating a lower computational complexity.

2.4 Algorithm

INPUT: intrusion attacks in 5G enabled IoT devices
OUTPUT: Accuracy of intruding attacks

```
Step 1: Initialize the Deep Reinforcement Learning agent with appropriate hyperparameters.
Step 2: Create a state space to represent the current environment.
Step 3: Define a reward function that rewards the agent for successful intrusion detection and penalizes it for false positives.
Step 4: Train the agent to recognize patterns of malicious behavior by providing it with labeled intrusion data.
Step 5: As the agent learns, adjust the reward function to further refine the agent’s understanding of malicious behavior.
Step 6: Test the agent on unseen data and measure its performance.
Step 7 Iterate and repeat steps 4 – 6 until the agent reaches an acceptable level of accuracy.
```

The aim of Deep Reinforcement Learning is to learn an optimal policy, and maximize the discounted total reward achieved from each state.

$$Q(s_{t,a_t})= (1-\alpha_t)Q(s_t,a_t)+\alpha_t) + \alpha_t(r_{t+1} + \gamma max_a Q(s_{t+1},a') \tag{4}$$

By taking into account the pair with the highest Q-value, Q-learning constantly aims to select the best course of action. In particular, DRL algorithms are excellent at resolving issues with messaging and mobile networks.

The proposed work was implemented using Google Colab and TensorFlow, with a hardware configuration comprising an Intel i5 10th generation processor, 8GB RAM, a 1TB HDD, and Windows 10 OS. The algorithms were tested on the training sets through empirical experiments.

2.5 Statistical Analysis

The proposed work underwent statistical analysis using the IBM SPSS software. This, coupled with an experimental analysis, was employed to compute the mean and standard deviation of the dependent variables – security, latency, accuracy, and privacy – in relation to the independent variables: sensor ID, sensor cycle, battery level, temperature, and time. A lightweight consensus algorithm, the Practical Byzantine Fault Tolerance (PBFT) (Tanwar 2021), which eschews proof-of-work and resource-intensive mining, was utilised to aid the implementation of the blockchain.

3 RESULTS

The performance of the proposed CNN model was juxtaposed against the DRL algorithm. The CNN model reported a mean accuracy of 84.63%, whereas the DRL algorithm achieved 70.70%. Despite the observed variance in accuracy rates, this study determined that there wasn't a statistically significant difference between the two models' performance, evidenced by a difference of 0.405 (P>0.05). The findings indicate that the proposed CNN model surpassed the DRL algorithm in classification accuracy.

Table 1 details the algorithms under comparison. The accuracy of the Deep Reinforcement Learning network stands at 70.70%, whilst the Novel Convolutional Neural Network's accuracy is 84.63%. Evidently, the Convolutional Neural Network outperforms Deep Reinforcement Learning in terms of accuracy.

Table 2 presents statistical calculations for both the Convolutional Neural Network and the DRL algorithms, encompassing metrics such as mean, standard deviation, and mean standard error. The analysis denotes that the CNN boasts a significantly superior mean value, 84.63, compared to DRL's 70.70.

Table 3 depicts the statistical analysis comparing the Convolutional Neural Network and Deep Reinforcement Learning. The latter's accuracy is 70.70%, while the Convolutional Neural Network's accuracy peaks at 91.27%. Nonetheless, the study discerned no statistically significant difference between the two groups.

4 DISCUSSION

This research examined the potency of a novel Convolutional Neural Network (CNN) architecture in tandem with a Deep Reinforcement Learning (DRL) algorithm and a blockchain security framework to detect and avert intrusion attacks in an IoT-centric

Table 1: The Accuracy rate for Convolution Neural Network with N=10 sample datasets in comparison with Deep Learning Reinforcement algorithm with the same sample size.

Sl.	Test size	CNN	DRL
1	Test size 1	76.13	67.91
2	Test size 2	76.43	68.23
3	Test size 3	77.56	68.56
4	Test size 4	82.95	69.99
5	Test size 5	85.37	69.14
6	Test size 6	87.01	69.87
7	Test size 7	88.76	70.01
8	Test size 8	90.13	72.08
9	Test size 9	90.78	75.11
10	Test size 10	91.27	76.13

Table 2: Group statistics of CNN compared with DRL algorithm in grouping with iterations of sample size 10, Mean =84.63, standard deviation=0.70711, error mean=0.15811.

Algorithms (accuracy)	Sample (N)	Mean	Standard deviation	Standard mean error
Novel Novel Convolutional Neural Network	10	84.63	6.03442	1.90825
Deep Reinforcement Learning	10	70.70	2.85588	0.90311

Table 3: The independent sample tests of accuracy for CNN in comparison with DRL are kind of significantly different from each other. There is significant difference of 0.405 (P>0.05) ensures the two groups are not significant.

accuracy	Leven’s test for equality variance		Test for equality of means					95% of the confidence interval of the difference	
	f	sig	t	df	Sig (2-tailed)	Mean difference	Std. error difference	upper	Lower
Equal variance assumed	8.058	0.011	6.601	18	0.405	13.9360	2.11117	18.371	9.500
Equal variance not assumed			6.601	12.839	0.405	13.9360	2.11117	18.502	9.369

setting. A comparative study was conducted with extant models that utilise Deep Reinforcement Learning to gauge if our suggested model could amplify detection precision. Experimental findings revealed that our model, underpinned by the CNN architecture, attained an accuracy rate of 84.63%, marking a substantial leap from the 70.70% secured by the Deep Reinforcement Learning model. This insinuates that the amalgamation of CNN, DRL, and a blockchain security framework is proficient at pinpointing and thwarting intrusion attacks in IoT-driven systems.

"The Resource Allocation for Reliable Low Latency Communication in 5G Intelligent Networks" as posited by Tekchandani et al. (2022) substantiates that DRL trumps primary techniques in terms of resource consumption and drop likelihood. To bolster the service quality in a 5G-fuelled smart grid, Qi and Liu (2018) championed the adoption of DRL to devise a dynamic strategy for network slice resources.

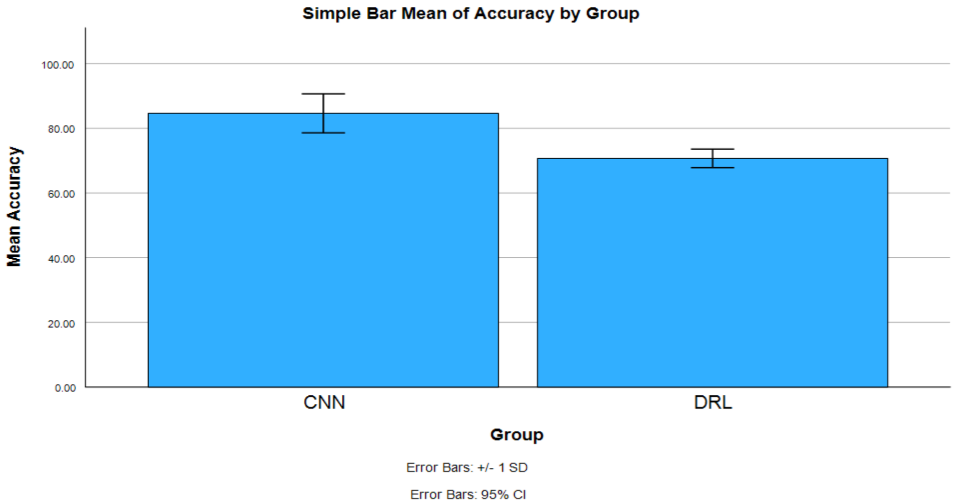

Figure 1: Comparing the accuracy of the CNN to that of the DRL algorithm has been evaluated. The Proposed method has a mean accuracy of 84.63 percent, whereas the DRL classification algorithm has a mean accuracy of 70.70 percent. The CNN prediction model has a greater accuracy rate than the DRL model. This study has found that there is a statistically not significant difference between the study groups with a difference of 0.405 (P>0.05).

This approach is nimble enough to adapt promptly to shifts in network demand, thereby optimising resource allocation. Li et al. (2018) put forth the application of DQN-based 5G-V2X to refine 5G-centric site allocation, primarily aiming to surmount the challenge of base station allocation. To carve out an adaptive decision-making stratagem for the initial window in 5G MEC, Yang et al. (2021) leveraged DQN. Their blueprint excels at boosting flow completion while concurrently curbing congestion.

Notwithstanding the optimistic results exhibited by the proposed model, it's imperative to acknowledge certain inherent constraints. The model's processing speed tends to decelerate owing to the incorporation of maxpool layers. Moreover, CNN models necessitate an ample volume of training data. Though adept at detecting an array of threats, the security framework isn't ideally streamlined for environments with restricted bandwidth. To circumvent these impediments, prospective enhancements might encompass the formulation of advanced firewall solutions to curtail data traffic and refine the security framework to facilitate superior bandwidth utilisation.

5 CONCLUSION

This study underscores the superior precision and accuracy of the Novel Novel Convolutional Neural Network (CNN) coupled with a blockchain security framework in forecasting intrusion attacks when juxtaposed with the Deep Reinforcement Learning (DRL) technique. The recorded accuracy for DRL stood at 70.70%, whereas the Novel Novel CNN method boasted an accuracy of 84.63%. A discernible difference of 0.405 (P>0.05) between the two methodologies ratifies the heightened accuracy of the Novel Novel CNN in predicting Quality of Service (QoS) as opposed to the DRL technique. Employing CNNs for intrusion detection offers a promising avenue, enhancing the precision of security frameworks. This is achieved by presenting a more detailed portrayal of network traffic, which subsequently augments the fidelity of intrusion prognostications.

REFERENCES

Zhang, J.; Pan, L.; Han, Q.-L.; Chen, C.; Wen, S.; Xiang, Y. (2021) Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA J. Autom. Sin. 9, 377–391

Lee, I. (2020) Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Futur. Internet, 12, 157

Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. (2020) Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory, 101, 102031

Mahapatra, S., Vickram, A. S., Sridharan, T. B., Parameswari, R., & Pathy, M. R. (2016). Screening, production, optimization and characterization of β-glucosidase using microbes from shellfish waste. 3 Biotech, 6, 1-10.

Azumah, S.W.; Elsayed, N.; Adewopo, V.; Zaghloul, Z.S.; Li, C. (2021) A deep lstm based approach for intrusion detection iot devices network in smart home. In Proceedings of the IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 26–31 July 2021.

Thakkar, A.; Lohiya, R. (2021) A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. Arch. Comput. Methods Eng, 28, 3211–3243.

Li, Y.; Zuo, Y.; Song, H.; Lv, Z. Deep learning in security of internet of things. IEEE Internet Things J. (2021); early access. (CrossRef) 7. Idrissi, I.; Boukabous, M.; Azizi, M.; Moussaoui, O.; El Fadili, H. Toward a deep learning-based intrusion detection system for IoT against botnet attacks. IAES Int. J. Artif. Intell. (IJ-AI) 2021, 10, 110.

Venkatraman, S.; Surendiran, B. (2019) Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems. Multimedia Tools Appl, 79, 3993–4010.

Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.-K.R. (2020) Consumer IoT: Security vulnerability case studies and solutions. IEEE Consum. Electron. Mag, 9, 17–25

Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A (2020) Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics, 9, 1177.

Wang, X.; Zhao, Y.; Pourpanah, F. (2020) Recent advances in deep learning. Int. J. Mach. Learn. Cybern, 11, 747–750.

Abu Al-Haija, Q.; Zein-Sabatto, S. An efficient (2020) deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics, 9, 2152.

Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. (2021) A systematic review on Deep Learning approaches for IoT security. Comput. Sci. Rev. 2021, 40, 100389

Stefanos, T.; Lagkas, T.; Rantos, (2022) K. Deep learning in iot intrusion detection. J. Netw. Syst. Manag. 2022, 30, 1–40.

Deena, S. R., Kumar, G., Vickram, A. S., Singhania, R. R., Dong, C. D., Rohini, K., ... & Ponnusamy, V. K. (2022). Efficiency of various biofilm carriers and microbial interactions with substrate in moving bed-biofilm reactor for environmental wastewater treatment. Bioresource technology, 359, 127421.

R. Pavaiyarkarasi, T. Manimegalai, S. Satheeshkumar, K. Dhivya and G. Ramkumar, (2022)"A Productive Feature Selection Criterion for Bot-IoT Recognition based on Random Forest Algorithm," 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), Indore, India, 2022, pp. 539-545, doi: 10.1109/CSNT54456.2022.9787583.

K. Biswas and V. Muthukkumarasamy, (2016) "Securing smart cities using blockchain technology", 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), pp. 1392-1393, 2016.

D. Han, H. Kim and J. Jang, (2017) "Blockchain based smart door lock system", 2017 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1165-1167, 2017.

Dorri, S. S. Kanhere and R. Jurdak, (2017) "Towards an optimized blockchain for iot", Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173-178, 2017.