Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 17 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i17.42805

PAPER

Deep Learning Algorithms in Mobile Edge with Real-Time Abnormal Event Detection for 5G-IoT Devices

J. Praveenchandar[1](✉), S. Vinoth Kumar[2], A. Christopher Paul[3], M. A. Mukunthan[2], K. Maharajan[4]

[1]Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India

[2]Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Tamil Nadu, India

[3]Department of Information Technology, Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India

[4]Department of Computer Science and Engineering, School of Computing, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India

praveenjpc@gmail.com

ABSTRACT

IoT is becoming increasingly popular due to its quick expansion and variety of applications. In addition, 5G technology helps with communication and network connectivity. This work integrates C-RAN with IoT networks to provide an experimental 5G testbed. In a 5G IoT environment, this experience is utilized to enhance both perpendicular and flat localization (3D localization). DRCaG, an acronym for the proposed model, stands for a deep, complicated network with a gated layer on top. The performance of the proposed model has been demonstrated through extensive simulations in terms of learning reduction, accuracy, and matrix disorientation, with a variable signal-to-noise ratio (SNR) spanning from 20 dB to + 20 dB, which illustrates the superiority of DRCaG compared to others. An online, end-to-end solution based on deep learning techniques is presented in this study for the fast, precise, reliable, and automatic detection of diverse petty crime types. By detecting tiny crimes like hostility, bag snatching, and vandalism, the suggested system may not only identify unusual passenger behavior like vandalism and accidents but also improve passenger security. The solution performs admirably in a variety of use cases and environmental settings.

KEYWORDS

localization, navigation, positioning accuracy, 5G, IoT, deep learning, DRCaG, precision

1 INTRODUCTION

5G has been creating new standards even though it is still in the testing phase. The size of the transition that 5G [1] will bring about contributes to a certain set of laws that govern the entire global communication network. Additionally, the IoT is developing, and a number of its user organizations are beginning to prepare for 5G. This is reasonable given the incredible benefits that 5G offers, including the availability of resources, reduced latency, a more seamless user interface, the ability to alter and adapt entire networks without affecting operations, and a significant increase in velocity.

Praveenchandar, J., Kumar, S.V., Paul, A.C., Mukunthan, M.A., Maharajan, K. (2023). Deep Learning Algorithms in Mobile Edge with Real-Time Abnormal Event Detection for 5G-IoT Devices. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(17), pp. 59–71. https://doi.org/10.3991/ijim.v17i17.42805

Article submitted 2023-05-04. Revision uploaded 2023-07-03. Final acceptance 2023-07-05.

Researchers are worried about how 5G will affect the security of communication between IoT devices. They are aware that crucial economic activity may be significantly impacted by hackers. The fundamentals of IoT architecture are the basis of this problem. For cybercriminals, any device logged onto the network presents a potential target. Big enterprises that use the design of the Internet of Things do not have a clear understanding of the complete network due to the substantial number of gadgets in the system. This is concerning because if criminals find a hole in one device, they might damage the current network. Additionally, as a result of the current situation, as many as 80% of these firms anticipate a considerable growth in the future in terms of the quantity of devices in their connected devices. In addition to the fundamental security concerns with IoT, 5G complicates matters. The data transmission over the network may be intercepted by criminals and hackers, causing more problems than what we already see with 4G networks. Given the flaws in 5G and IoT facilities, security can be ensured in many ways.

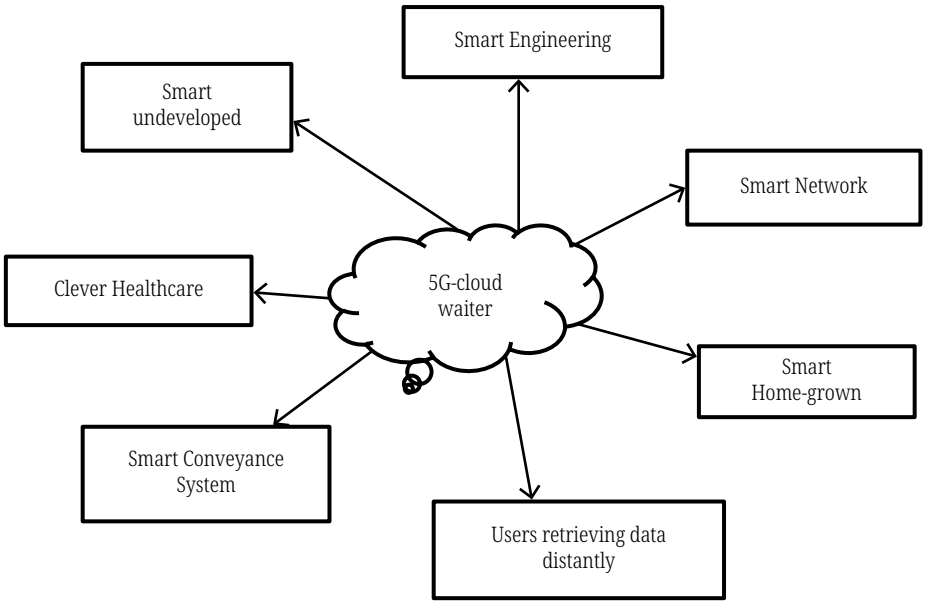

Fig. 1. 5G-enabled IoT environment network architecture

Even though it offers a speedier system with more volume to address connectivity requirements, 5G is essential for IoT in Figure 1. The frequency range that mobile phone technology employs to transfer data is expanded by the 5G spectrum. Due to the large amount of available space, mobile networks' overall bandwidth increases, allowing for the connection of additional devices. 5G unquestionably has to have control over how quickly the network and network structure respond to address current difficulties. Neural networks (NNs) have gained a lot of momentum as a competitive alternative to conventional categorization algorithms in wireless networks of the 5G and B5G. In 5G and B5G mobile networks, NN-based classifiers [2], which are feature-based, are frequently employed to solve AMC issues. Because of its more lightweight and adaptable design, its application in the IoT is particularly promising.

The process of classifying a signal's modification scheme is known as AMC. It is a fundamental method of non-cooperative telecommunication and functions as a step between the signal-receiving and signal-demodulation processes. It is important to note that the hypothetical Internet of Things employs a separate set of communication technologies, such as wireless sensor networks. As a result, fog calculation

played a part in this situation [3]. Through a decentralized networking and computing structure, fog computing, also known as fogging, primarily entails the efficient distribution of information, delivery, storage, and software between data sources and the public internet. The Paper's Contribution is as follows:

- A unique deep learning method based on autoencoders is used to detect network assaults.
- For implementation, several DL procedures are used.
- For the implementation, a new benchmarking dataset is utilized.
- The work has been compared to the current framework in an evaluation.

The structure of this essay is as follows. The review of the literature based on several intrusion detection organizations is described in Section 2 of this article. The Deep Learning Algorithms in 5G Wireless Mobile are described in Section 3. Section 4 presents the platform implementation information as well as the simulations performed to evaluate the effectiveness of our suggested approach. Section 5 brings our article to a close.

2 RELATED WORKS

Hu, N., Tian, Z., Lu, H., Du, X., et al. [4] research on intrusion detection based on artificial intelligence has garnered a lot of attention recently due to the quick growth of machine learning technology. Misuse identification, finding anomalies, and hybrid prevention are the three basic IoT intrusion detection techniques. The terminal security problem is not covered here since the study in this article is primarily focused on the network intrusion detection issue related to IoT. The fundamental concept of interruption finding equipment is to ascertain by looking at the hidden components of the selected data, such as computer logs, network usage, and other data, whether an attack incident can be determined. Many intrusion detection solutions based on artificial intelligence techniques have been proposed, with the three main types being unsupervised machine learning, machine learning under supervision, and deep learning. This is because machine technology has inherent advantages in the analysis of information.

Haider, N., Baig, M. Z., & Imran, M et al. [5] The 17 primary threats and areas and potential solutions for the security design of 5G networks were highlighted by the 3GPP specifications Group Services and Techniques Aspects (TSG SA3) in their release 13 document. Release 15 (R15), which was released in June 2019, then outlined the security architecture, practices, and specifications for 5G networks. While the next R16 and R17 will concentrate, R15 offers security criteria for standalone and non-standalone improved wireless broadband circumstances based on security demands for massive machine-type communication and ultra-reliable low-latency textual communication. The unique safety features seek to give E2E security together with the ability to accommodate different authentication systems in order to enable protection for the Service Oriented Architecture (SBA) in 5G.

Tsai, Y. H., Chang, D. M., & Hsu, T. C. et al. [6] DL networks are currently typically installed on cloud servers, taking into account computer power. However, in this case, to carry out event detection duties, the acquired data must be sent to the cloud. It frequently causes postponements in the model of increased communication costs, privacy worries, and cloud computing, making it impossible to complete the assignment on time. End device communication had been proposed to be made possible through a machine-to-machine service platform. This approach significantly reduces network

traffic and speeds up overall performance thanks to the participation of end stations. Only basic learning algorithms can be done due to the end device's lack of computation and storage capacity, and high reliability may not ultimately be attained.

Santos, J., Wauters, T., Volckaert, B., et al. [7] The Lightweight M2M, a device administration procedure shaped by the Open Mobile Alliance, is used in M2M and sensor network settings. LwM2M is based on network and safety guidelines from the Internet Engineering Task Force, and it was developed by a group of industry professionals at the OMA's Device Management Working Group. To fully realize the promise of the Internet of Things, a single standard for managing small, low-power devices is required. OMA LwM2M seeks to meet this demand. The Constrained Application Protocol (CoAP), an effective secure data transfer standard, serves as the foundation for the LwM2M protocol. As previously indicated, the one M2M management devices and safety requirements, which are the primary goals of the LwM2M protocol, are followed by the proposed cloud computing architecture.

Fan, Y., Li, Y., Zhan, M., Cui, H., & Zhang, Y. et al. [8] IDS can be broadly classified into rule-based and anomaly-based detection techniques. Many academics are intrigued by applying ML algorithms to create anomaly-based IoT IDS. A self-encoder-integrated online unsupervised intrusion detection system that has undergone testing in IoT devices and IP cameras Continuous Variation Auto Encoder (CVAE) was offered as the foundation for an uncontrolled anomaly NIDS for the IoT, while Multi-Layer Perceptron (MLP) was used in an off-line IoT IDS as an unsupervised Artificial Neural Network (ANN). They use net packet traces as the basis for their research, and they frequently detect DoS attacks in IoT networks.

Mahdi, M. N., Ahmad, A. R., Qassim, Q. S., et al. [9] The important articles and research cited in the search results were chosen and categorized based on two factors: (1) use a total of three passes in the filtering procedure to remove unnecessary and duplicate articles and exclude irrelevant items using their titles, and (2) use three rounds in the process of categorization to classify the important articles and literature cited in the search outcomes. Perform the initial examination after carefully analyzing the results of the limited search. After that, the 5G and 6G are used for a second screening of the selected articles. In order to ensure that only the latest and highly relevant scientific studies that enhance the potential of 5G and 6G are collected, exclusions are created. The emphasis is on including all scientific contributions and articles that follow the requirements for this study.

Cui, L., Yang, S., Chen, F., Ming, Z., et al. [10] The study of IoT intelligent machines has advanced significantly. We may therefore draw the conclusion that machine learning support for IoT can be beneficial. Given that neural networks may provide practical ways to extract the information and characteristics hidden in IoT data, their usage in IoT enables users to acquire deep insights and create efficient intelligent devices. In this paper, the usage of deep neural networks for the IoT is examined by illustrating potential collaboration using use case scenarios. In the interim, we investigate the data science and IoT connectivity gaps that now exist to find challenges and possible future solutions.

El Boudani, B., Kanaris, L., Kokkinis, A., et al. [16] DL techniques have been widely employed in the fingerprint-based strategy to improve localization by gleaning from a sparse radiomap catalogue that frequent patterns. Due to its resilience and great accuracy, it has been quite popular recently, especially among academics studying indoor localization. Recent developments in 2D localization and multi-floor localization use supervised and unsupervised deep learning methods. The location of the node was recently examined using Convolutional Neural Networks on IoT-Sensor Systems. The 2D localization problem was transformed into a 3D image tensor recognition problem by the simulation's designers. To create the 3D tensor, a 2D matrix of RSS data and 1D kurtosis were combined.

3 METHODS AND MATERIALS

The network is made up of two subsystems: a real-time massive information processing system based on a combination of system based on a deep artificial neural networks, as well as an ambient reflector transmission network for real-time data transport. The real-time big data analysis platform is at the center of monitoring and diagnosing the bodily condition of users, even if the real-time data delivery system provides excellent data transfer security. To assure reliable data transfer, a collaborative ambient backscatter transmission approach is developed [11]. This system for immediate data transfer is based on ambient scattering transmission.

3.1 Transmission design

Let's say that $|YQT|\ 2 = 1$ and that $Q(M)$ denotes the principal gen signal sent from PT to PR at the kth sign in the nth chunk. Let $Q(m)$, which is presumed to be corrected in this letter, stand for the signal strength for the main reception in the nth block, the broadcast signal at PT to the main receiver is provided by

$$YQT = \sqrt{Q(M) * r(m,l)} \tag{1}$$

Let's say that $YBE\ (m,l) = 1$ and that $r\ (m,l)$ denotes the returned data signal delivered from BD to CR at the nth representation in the kth block. At BD, the communication signal is provided by

$$YBE(m,l) = \sqrt{l_2(m)} * YQT * r(m,l) \tag{2}$$

If $xqs\ (m,l)$ represents the signal that was received at the yql for the kth symbols in the nth block, the resultant signal is represented by

$$xqs(m,l) = \sqrt{l_1(m)} * yql(m,l) + \sqrt{g_1(m) * r(m,l) + mqr(m,l)} \tag{3}$$

For decoding the main data stream, the immediate signal to interruption plus noise ratio ($RJMS$) is provided by

$$RJMS_{qr} = \frac{qh_1(m)}{q_{\partial} l_4(m) g_2 + 2} \tag{4}$$

And the matching feasible principal information signal transfer rate between QT and PS is provided by

$$S_{qr} = log_1(2 + RJMS_{qr}) \tag{5}$$

The signal that was picked up at CR is given by $x_{cs}(m,l)$, where $ql(m,l)$ denotes the signal received at the CS for the kth letter in the nth wedge.

$$X_{cs}(m,l) = \sqrt{l_2}(m) * yql(m,l) + \sqrt{g_2(m)} * \sqrt{yql(m,l)} + mds(m,l) \tag{6}$$

Where the normalized multiplicative noise generated at CS is represented by $RJMS_{qr}$. In this study, we suppose that the CR successively cancels interference (SIC) to decelerate the incoming signal.

$$RJMS_{qr} = \frac{qh_1(m)}{\partial qh_1(m) l_1(m) + 2} \tag{7}$$

It is given as the major data signal's feasible velocity of transmission from PT to BD

$$S_{DS} = log_1(2 + RJMS_{qr}) \tag{8}$$

The $\partial qh2$ can be removed from (6) if the $l(m)$ can be decoded. The *RJMS* is given by ten for deciphering the backscatter data stream.

$$RJMS_{qr} = \partial qh2(m) l(m) \tag{9}$$

It gives the returned data signal received at CS's equivalent feasible transfer rate.

$$S_{QR}^{d1} = \frac{\partial qh2(m) l(m)}{Ph_2(m) + 1} \tag{10}$$

3.2 Advanced learning methods

- Algorithms used by machine learning systems enhance their output in response to experience. Because ML models can be expanded to accommodate fresh limitations and inputs without having to start from scratch and because they can resolve mathematically challenging equations, machine learning will eventually replace conventional optimization techniques in many fields. As we can see with computer systems today, ML models can easily be modified to fit new circumstances.
- DL, a branch of machine learning that has received a lot of interest in computer vision over the past decade, has led to the discovery of new, more effective game tactics without the time- and money-consuming need for handcrafted engineering features.
- DL automates feature abstraction from enormous data sets using neural networks and later uses these characteristics to organize inputs, variety judgments, or create new data.
- After the introduction of Visualize, a curated library of over 11 million photos divided into 11,000 categories and used to train ML image classification models, research on DL for machine learning flourished.
- Due to the lack of appropriate data sets for 5G network activity due to the newness of the technology and its limited deployment, several authors have turned to simulations.
- The models of service demand may alter as a result of 5G and slice-based schmoozing. However, due to the possibility of disclosing confidential or customer information, only a few researchers have access to comprehensive and representative information from broadcastings corporations.

3.3 Algorithms for deep learning in 5G wireless mobile

In the 5G-based IoV, CNN chooses the networks. The algorithm of the jellyfish was used to choose the vehicle-to-vehicle twosomes. The development of a perpendicular handover decision using 5G mmWave, LTE, and DSRC in IoT included dynamic Q-learning and FCNN [15]. Handover failure, handover success likelihood, redundant

transfer, productivity, lost packets, and delay is the measures used to assess CNN's performance.

The exploration of vehicle crowd sense was inspired by the lack of comprehensive studies on data protection and privacy protection. In the 5G-powered IoV, vehicular crowd sensing, driven by blockchain and based on DRL, is used to ensure user privacy and safety. To reduce latency and increase blockchain security, active miners and transactions are chosen using the DRL. The two-sided matching algorithm allows nonorthogonal multiple access subchannels. It is discovered that this system offers maximal security, defense against common threats, and preservation of privacy and authenticity. The application of federated instruction in 5G-powered IoV for license plate recognition was driven by the privacy risk associated with centralized training models. Instead of using a server, personal mobile phones were used to collect information for the modelling. The federated learning strategy was shown to protect privacy, have excellent accuracy, and have efficient communication costs.

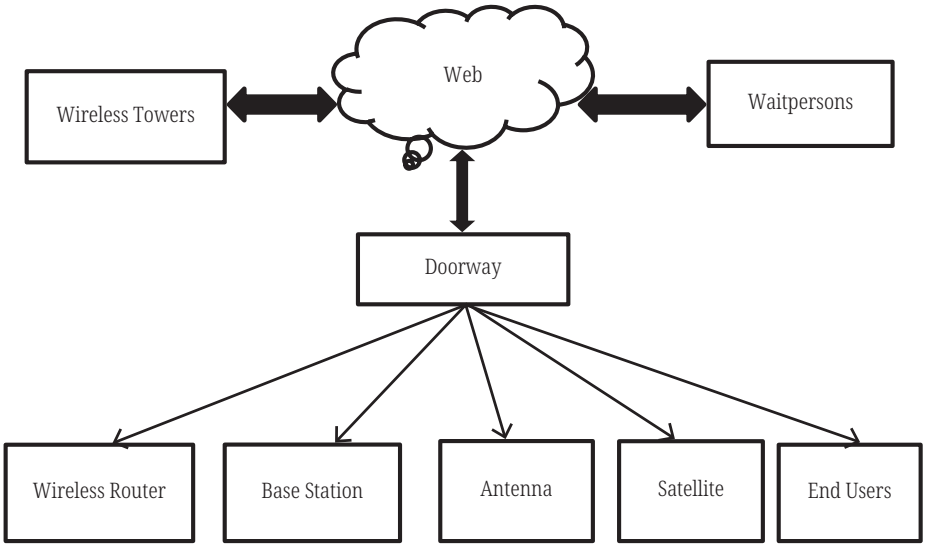

Fig. 2. Summary of the DRCaG concept

Figure 2 shows a typical IoT system for the DRCaG concept that is being taken into consideration. An electronic system is made up of terminal nodes, which are detectors or intelligent objects with embedded CPUs and other connection hardware. Network pathways, one or more information processing centres, and other elements are also included in IoT networks. IoT architectures vary depending on the software being used and, as a result, display high levels of variability depending on particular needs. Effective wireless connectivity between component devices in IoT systems is one of the network layer's issues.

The system's structure and architecture sometimes call for the employment of a variety of modulating formats, which makes it difficult for the earpiece to classify indications. Collectively, these have an impact on the network's overall complexity. This work makes an effort to use a trained, lightweight DL-based group classifier to address a significant power-constrained IoT-based network communication constraint.

3.4 The mobile edge's DL concerns for 5G deployment

The difficult taxonomy for using DL in 5G systems is introduced in this part and serves as the foundation for this study. This taxonomy, which is depicted in Figure 3,

is used to group research publications into categories based on how they apply deep learning techniques to the network activities covered in this paper.

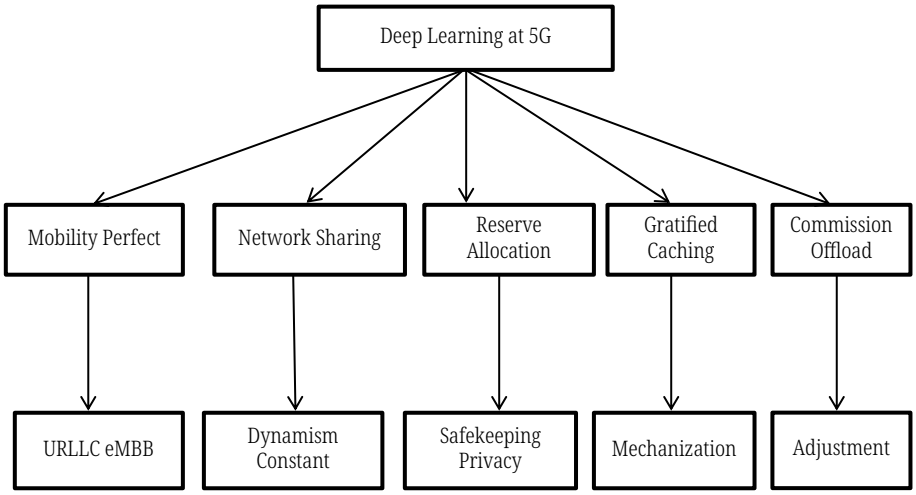

Fig. 3. The difficulties with using deep learning for network management at the edge of 5G systems

This section describes the usage of DL to address operational problems at the mobile edge. By utilizing the innovations covered in the previous section, mobile edge computing, which has the advantage of being close to customers, can accomplish the aims of the 5G networks for low latency (URLLC), high bandwidth (eMBB), and high availability (mMTC).

In order to decrease delay and combine locally important evidence, 5G networks provide fascinating issues that need to be solved at the mobile edge [12, 13]. To handle several issues in 5G connectivity in specific, a lot of those need automated management. Edge computing devices can benefit from being near the user by using DL for an increasing variety of complex tasks when carried out in edge computing devices close to the end user instead of the main network solutions incorporating DL for 5G offer greater efficiency. For example, combining portable edge computing with 5G networks creates a smooth connection between edge computing and current cloud services to enable novel applications.

DL has a wide range of potential networking applications, but this study concentrates on a few crucial ones: Using forecasting traffic within computing edges on mobile, responsive distributing resources delegating duties from close-by end devices, excellent service assurances, effective energy consumption, data safety and secrecy, network architecture norms, and robots, predictive caching for lowering delay. Although they can appear to be distinct jobs, they are closely related. Before DL is completely usable in the 5G mobile edge, there are still several obstacles to overcome, many of which apply to machine learning systems in general.

4 IMPLEMENTATION AND EXPERIMENTAL RESULTS

The experimental setup, the DRCaG model's simulation outcomes, and its performance in comparison to the network are all covered in this part [14, 16]. The effectiveness of the suggested solution for the problem at hand is also assessed.

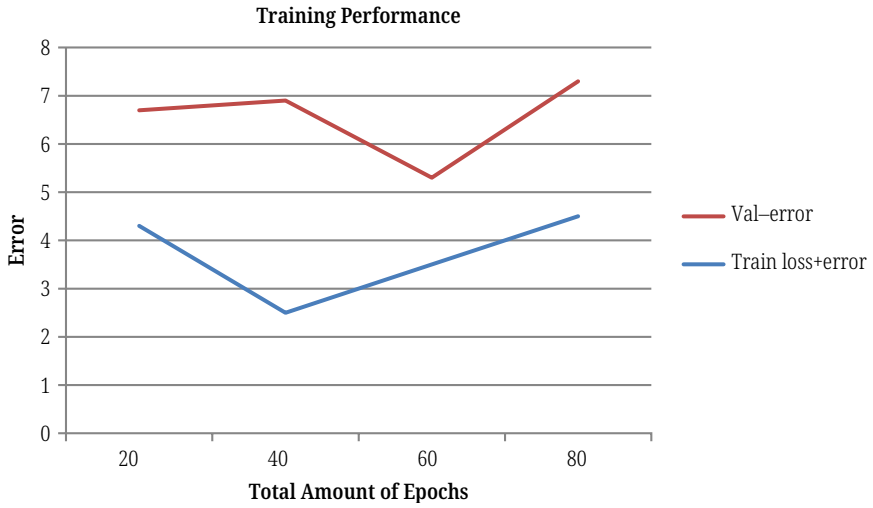

Fig. 4. Models under consideration for training loss DRCaG model

The presentation of the suggested DRCaG model is investigated as a potential replacement for current models like the 4-layered CNN and LSTM. For learning loss and precision, these models' efficiency has been compared. The 4-layered CNN, LSTM, and DRCaG replicas' training loss and validation error are shown in Figure 4.

Table 1. Correctness evaluation

Correctness (%)			
SNR (db)	CNN (%)	LSTM (%)	DRCaG (%)
–30	14.01	15.10	16.01
–20	31.00	31.00	32.00
0	78.00	70.00	86.00
+20	83.00	84.00	89.00
+25	83.00	84.00	91.00

Table 1 shows that the accuracy of the suggested DRCaG model, LSTM, and 4-layered CNN models at higher SNRs is 83%, 84%, and 91%, respectively. However, the training durations for the LSTM-based models were the shortest, taking about 19 mins for 160 epochs. The proposed DRCaG is considerably higher than the current models and can be utilized as a good substitute for applications that require little power.

4.1 Discussion about DRCaG model computational aspects

The biggest barrier to implementing conventional classifiers in IoT-based systems is their extensive processing needs. Although likelihood-based classification approaches are computationally demanding and therefore challenging for lightweight execution, they theoretically offer the best accuracy levels [17, 18]. Although conventional feature-based classifiers have nonlinear issues, they are light enough for applications in the IoT. Additionally, because features must be chosen while taking into account the specific modulation types, the classifier is less adaptable in real-world presentations. DL-based classifiers positively balance the need for a high level of correctness with reduced computing costs. Even in this case, training more complicated networks on bigger sets can significantly enhance performance, but it also requires more computing resources and can extend training timeframes.

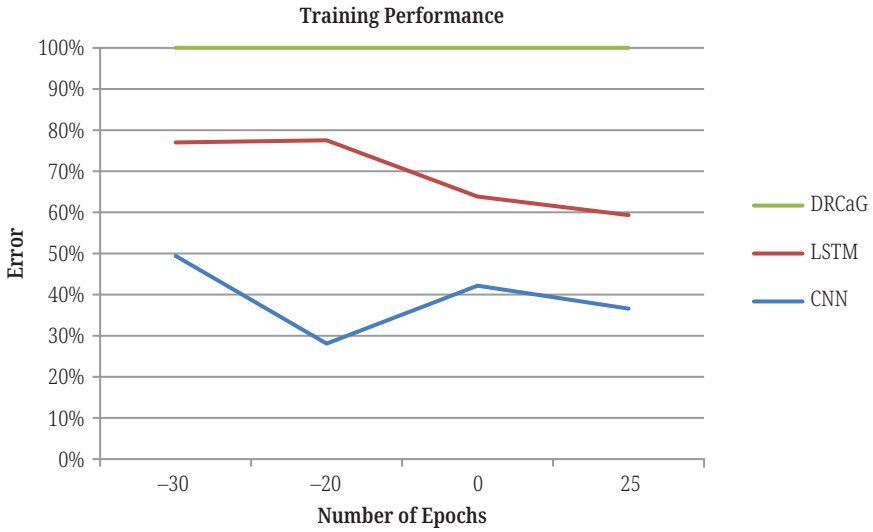

Fig. 5. Models with training loss are the 4-layered CNN model, the LSTM model, and the DRCaG prototypical

Figure 5 shows that for the models under discussion, the working out loss and authentication failure decrease as the number of epochs rises. Furthermore, it is noted that the suggested DRCaG model has higher training loss and authentication errors for fewer epochs than existing DL models. Nevertheless, it fared better than other models with an abundance of epochs.

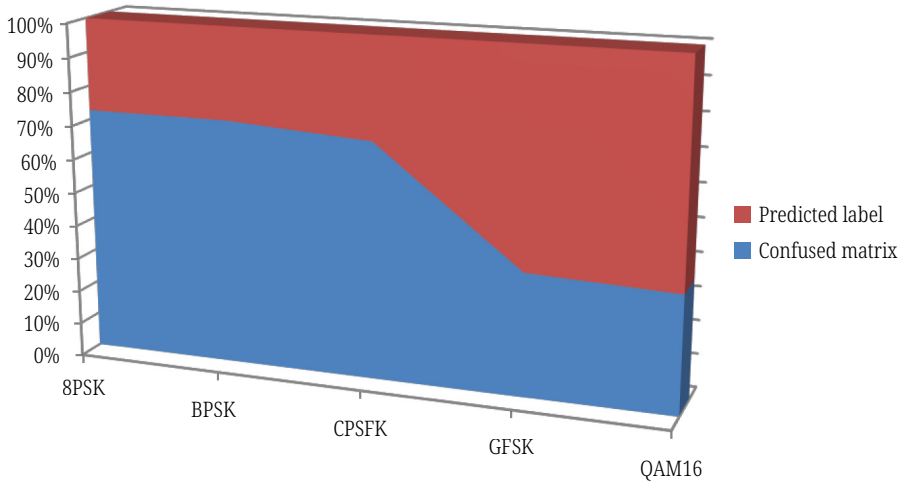

Fig. 6. DRCaG model confusion matrixes

Due to their unique signal properties, some modulation signals are undoubtedly more challenging to categorize. The DRCaG model's confusion matrix is shown in Figure 6. It may be inferred that DRCaG and each of the tested models significantly overclassified the 8-PSK and QPSK indication categories. As a result of the modulation scheme, they both can be accredited to the parallels in I/Q sample trends. With the use of a larger and more comprehensive dataset and additional micro tuning of prototypical hyper limitations, its accuracy can be increased even further. The suggested DRCaG exemplary for IoT-assisted wireless systems, however, shows promise and potential in the initial findings, which are indicative of this.

5 CONCLUSION

In the present investigation, we introduce an effective and secure IoT authentication solution for 5G network amenities. With the help of the optimal data, transmission network slices may be selected by 5G-IoT nodes while user access types are concealed thanks to a privacy-preserving slice choosing technique in the framework. Operators can establish an anonymous connection to the servers of 5G-IoT devices and set up a secure data channel to access locally reserved documents that have been stored on a remote server.

The usage of DL-based detectors for IoT is justified enough. An effectual model for this issue must strike a compromise between portability and accuracy. Due to its lightweight construction and increased accuracy, the suggested DRCaG model is a viable replacement for current DL models in IoT applications. Through comprehensive simulation, it has been addressed and shown that the suggested model is effective in terms of precision, confusion matrix, and simplicity. For IoT-assisted wireless networks for the system under study, the suggested model exhibits a 8% improvement in accuracy over the current models.

As a conclusion, we hope that the responses to our questionnaire will provide insight into the development and use of DL in mobile edge computing. These techniques might inspire further research and the deployment of scenarios that boost future network and service management.

6 REFERENCES

[1] Rajawat, A. S., Bedi, P., Goyal, S. B., Shukla, P. K., Jamal, S. S., Alharbi, A. R., & Aljaedi, A. (2021). Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation. *Mathematical Problems in Engineering*, 1–10. https://doi.org/10.1155/2021/2330049

[2] Roy, C., Yadav, S. S., Pal, V., Singh, M., Patra, S. K., & Sinha, G. R. (2021). An ensemble deep learning model for automatic modulation classification in 5G and beyond IoT networks. *Computational Intelligence and Neuroscience*. https://doi.org/10.1155/2021/5047355

[3] Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion detection system on IoT with 5G network using deep learning. *Wireless Communications and Mobile Computing*, 1–13. https://doi.org/10.1155/2022/9304689

[4] Hu, N., Tian, Z., Lu, H., Du, X., & Guizani, M. (2021). A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks. *International Journal of Machine Learning and Cybernetics*, 1–16. https://doi.org/10.1007/s13042-020-01253-w

[5] Haider, N., Baig, M. Z., & Imran, M. (2020). Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends. *arXiv preprint arXiv:2007.04490*.

[6] Tsai, Y. H., Chang, D. M., & Hsu, T. C. (2022). Edge computing based on federated learning for machine monitoring. *Applied Sciences*, *12*(10), 5178. https://doi.org/10.3390/app12105178

[7] Santos, J., Wauters, T., Volckaert, B., & De Turck, F. (2017). Fog computing: Enabling the management and orchestration of smart city applications in 5G networks. *Entropy*, *20*(1), 4. https://doi.org/10.3390/e20010004

[8] Fan, Y., Li, Y., Zhan, M., Cui, H., & Zhang, Y. (2020, December). Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. In *2020 IEEE 14th international conference on big data science and engineering (BigDataSE)* , pp. 88–95. IEEE. https://doi.org/10.1109/BigDataSE50710.2020.00020

[9] Mahdi, M. N., Ahmad, A. R., Qassim, Q. S., Natiq, H., Subhi, M. A., & Mahmoud, M. (2021). From 5G to 6G technology: Meets energy, Internet-of-Things and machine learning: A survey. *Applied Sciences*, *11*(17), 8117. https://doi.org/10.3390/app11178117

[10] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., & Qin, J. (2018). A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics*, *9*, 1399–1417. https://doi.org/10.1007/s13042-018-0834-5

[11] Liu, Q., Sun, S., Yuan, X., & Zhang, Y. A. (2021). Ambient backscatter communication-based smart 5G IoT network. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 1–19. https://doi.org/10.1186/s13638-021-01917-3

[12] McClellan, M., Cervelló-Pastor, C., & Sallent, S. (2020). Deep learning at the mobile edge: Opportunities for 5G networks. *Applied Sciences*, *10*(14), 4735. https://doi.org/10.3390/app10144735

[13] Sai Santhiya, D., Padmapriya, T., Salameh, A. A., Wildan, M. A., & Kishore, K. H. (2022). AI enabled-6G: Artificial intelligence for integration of 6G wireless communication. *International Journal of Communication Network and Information Security*, *14*(3), 372–379.

[14] Roy, C., Yadav, S. S., Pal, V., Singh, M., Patra, S. K., & Sinha, G. R. (2021). Research article an ensemble deep learning model for automatic modulation classification in 5G and beyond IoT networks. https://doi.org/10.1155/2021/5047355

[15] Almutairi, M. S. (2022). Deep learning-based solutions for 5G network and 5G-enabled Internet of vehicles: Advances, meta-data analysis, and future direction. *Mathematical Problems in Engineering*, 1–27. https://doi.org/10.1155/2022/6855435

[16] El Boudani, B., Kanaris, L., Kokkinis, A., Kyriacou, M., Chrysoulas, C., Stavrou, S., & Dagiuklas, T. (2020). Implementing deep learning techniques in 5G IoT networks for 3D indoor positioning: DELTA (DeEp Learning-Based Co-operaTive Architecture). *Sensors*, *20*(19), 5495. https://doi.org/10.3390/s20195495

[17] Alam, A., Das, A., Tasjid, M. S., & Marouf, A. A. (2021). Leveraging sensor fusion and sensor-body position for activity recognition for wearable mobile technologies. *International Journal of Interactive Mobile Technologies (iJIM)*, *15*(17), 141–155. https://doi.org/10.3991/ijim.v15i17.25197

[18] Shaikh, A. (2020). Advances in deep learning in mobile interactive algorithms and learning technologies. *International Journal of Interactive Mobile Technologies (iJIM)*, *14*(10), 4–6. https://doi.org/10.3991/ijim.v14i10.15369

7 AUTHORS

Dr. J. Praveenchandar, B.E., ME., PhD is working as an Assistant Professor (S.G) in the department of Computer Science and Engineering in Karunya Institute of Technology and Sciences, Coimbatore. He has got more than 15 years of teaching and research experience in various reputed engineering colleges in Tamilnadu in the field of Computer Science and Engineering, in specific Cloud computing and Big Data Analytics. He completed his BE (CSE), ME (CSE) & PhD (ICE) in Anna University, Chennai. He has published his research articles in many reputed SCI/Scopus/WoS indexing journals and presented his ideas in many international conferences. He has three international & Indian design patents and copyrights. He is the reviewer of many SCI indexed journals. His research interests include Cloud computing and Big Data Analytics (email: praveenjpc@gmail.com).

Dr. S. Vinoth Kumar is presently working as Associate Professor in the department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. He received his Bachelor of Engineering – Computer Science and Engineering from Anna University, Master of Engineering – Computer Science and Engineering from Anna University, Tirunelveli. He completed his PhD at Karpagam University, Coimbatore. His research interests include Image Mining, Data Mining, Networks and Cloud Computing. He published almost 20 papers in refereed international journals and presented 15 papers in national and international conferences. He is an active member of IAENG. He has visited various countries like South Korea, Malaysia and Singapore for Faculty Exchange Program on Academic Affairs (email: profsvinoth@gmail.com).

Dr. A. Christopher Paul is presently working as Associate Professor in the department of Information Technology at Karpagam Institute of Technology, Coimbatore. He received his Bachelor of Engineering – Computer Science and Engineering from Anna University, Master of Engineering – Computer Science and Engineering from Anna University, Coimbatore. He completed his PhD at Karpagam University, Coimbatore. His research interests include Image Mining, Data Mining, Networks and Cloud Computing. He published almost 10 papers in refereed international journals and presented 5 papers in national and international conferences. He is an active member of IAENG. He has visited various countries like South Korea, Malaysia and Singapore for Faculty Exchange Program on Academic Affairs (email: profachristo@gmail.com).

Dr. M. A. Mukunthan has about 22 years of experience in industry and teaching. He is currently serving in Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology. He completed PhD degree in the area of software quality metrics and analysis. He published more than 20 papers in international journals and presented his papers in various international and national conferences. He claimed 2 IPRs for different products. He is also acting as an editor and reviewer for reputed international journals. He is passionate involved in activities to facilitate about the career development of engineering students. He is the Life member of ISTE. His area of interest includes anti forensics, Cyber security, Cyber Forensics and Software Engineering (email: drmamukunthan@veltech.edu.in).

Dr. K. Maharajan is currently working as an Associate Professor in Department of CSE, Kalasalingam Academy of Research and Education (Deemed to be University), Krishnankoil. He did his Diploma in E.C.E in Arasan Ganesan Polytechnic, Sivakasi. He did Post Diploma in Advanced Electronics at ATI-EPI, Hyderabad. He did B.E (CSE) at PSR Engineering College, Sivakasi. He has done M.E (CC) at National Engineering College, Kovilpatti. He received PhD in Information Communication Engineering from Anna University, Chennai. His research interests span both data science, network science and Cloud Security. Much of his work has been on improving the understanding, design, and performance of parallel and networked computer systems, mainly through the application of unconventional computing methods, data mining, statistics, and performance evaluation. He is committed to helping students identify and develop their own passions while becoming successful and confident scholars and learners. He has an exceptional track record of research success with multiple published articles in highly indexed journals and conferences. He has more than 15 years of teaching and research experience. He is guiding seven research scholars in the domain of Computer Vision, AIML, and Cloud security. Currently he is the acting Associate HoD in the department of Computer Science and Engineering, School of Computing. He published more than 15 research papers in reputed journals (email: maharajank@gmail.com).