Periodicals of Engineering and Natural Sciences
Vol. 10, No. 2, March 2022, pp.128-137

ISSN 2303-4521
Original Research

Implement DNN technology by using wireless sensor network system based on IOT applications

Saif Saad Hameed[1], Haider Rasheed Abdulshaheed[2], Zaydon L. Ali [3], Hassan Muwafaq Gheni [4]
[1] College of Computer Science and Information Technology, University of Anbar, Iraq
[2] Computer Engineering Techniques Department, Baghdad College of Economic Sciences University, Iraq
[3] College of Political Science, Mustansiriyah University, Iraq
[4] Computer Techniques Engineering Department, Al-Mustaqbal University college, Iraq

ABSTRACT

The smart Internet of Things-based system suggested in this research intends to increase network and application accuracy by controlling and monitoring the network. This is a deep learning network. The invisible layer's structure permits it to learn more. Improved quality of service supplied by each sensor node thanks to element-modified deep learning and network buffer capacity management. A customized deep learning technique can be used to train a system that can focus better on tasks. The researchers were able to implement wireless sensor calculations with 98.68 percent precision and the fastest execution time. With a sensor-based system and a short execution time, this article detects and classifies the proxy with 99.21 percent accuracy. However, we were able to accurately detect and classify intrusions and real-time proxy types in this study, which is a significant improvement over previous research.

Keywords: Deep learning, Intelligent-IOT, Accuracy, DNN, WSN.

Corresponding Author:

Saif Saad Hameed
College of Computer Science and Information Technology
University of Anbar
Ramadi, Al-Anbar, Iraq
E-mail: dove_white84@uoanbar.edi.iq

1. Introduction

Ad hoc network architecture is used in Sensor Networks (WSN) to report events to a central base station (BS). By integrating a WSN and smart technologies, fast IOT communications are achievable [1] and [2]. In part to avoid network congestion, a WSN with IOT in a practical case must prioritize different types of data based on their importance [3]. There is a significant role for the IOT devices in area monitoring, where multiple IOT nodes process data and send it to a gateway or the cloud for further analysis of the collected data. It will be more expensive to transport data that is multi-dimensional (such as videos or time-series data). IOT networks with low bandwidth and low-power devices may not be able to handle frequent transmission at high data rates. In addition to [4], Intelligence may be added to a IOT using Machine Learning (ML) and Deep Learning (DL) approaches (IOT). In large-scale IOT networks, resource management is a significant issue that ML and DL can help solve [6]. When deep neural networks are used on IOT devices, new applications that can execute sophisticated sensing and understanding tasks could be developed to enable human-environment interaction [7]. The use of deep learning DNNs as controllers for deep Neural Networks (DNNs) has grown in recent years [8,10]. An intelligent structure is the main objective of this article.

2. Literature review

Large amounts of data are collected by sensor integrated IOT devices. One of the most difficult tasks will be to keep track of such vast amounts of data. In this section, we'll look at two of the most important approaches. The first question is how to select an appropriate DNN controller for I-IOT network congestion, and the second question Rather than using the old way like in [11,12], how can we locate a DNN-based clustering technique? On the topic of DNNs in various applications, this section includes contains recent research. DNNs were used as part of a mobile show's channel capacity state information in order to increase connection capacity and enhance energy efficiency. An attempt was made by. [13] to enhance DNN bandwidth. To improve QoS and increase the network's security [14] suggested to use a clustering technique based on the deep learning DNN technology and an optimization of signal strength in an industry IOT network. Adding recurrent feedback into the DNN structure makes it much more powerful. According to the work of [14], (ReDNN) was developed to learn the interpretations of an image's spectral, spatial, and temporal features. Remote sensing picture analysis of this structure was successful. To alleviate traffic congestion [15] recommended using CSI and DNN built on (LTE) for parking. Indoor person tracking with deep RNN and WSN has been demonstrated by [16] to improve the estimation of position collected by wireless sensors. While developing the Concurrent Repeated Convolutional Neural Network for mobile IOT and sensors (PRDNN) [17]. Also [18] suggested a hybrid technique employing DNN and RNN that outperforms than DNN in estimating the salvage value of predictive health management technology. Numerous researchers are engaged in efforts to enhance the focus of NNs. For example, every RNN neuron in a layer can be empowered by a simple effective (EleAttG) that can be applied to an RNN block. with concentration effectiveness. Real-time wireless localization has been made easier with the development of the DL-RNN model by [19], which utilizes two recurrent neural networks (RNNs) to improve wireless fingerprinting localization performance. A number of algorithms have been proposed by researchers to enhance the DNN's ability to pay attention in the training process [16,18]. Additionally, clustering techniques are extremely useful in reducing network congestion in I-IOT networks.

A protocol known as Congestion-Conscious Clustering & Routing (CCR) was developed by [20] to help alleviate network congestion. The protocol's goal was to meet the QoS requirements of extending the life of the network and sending more packets. Overloaded networks benefit from the bandwidth allocation method, which prioritizes high-priority traffic over lower priority traffic. [21] employed Back Propagation Networks to solve the cluster head detection algorithm in MIMO sensor networks. (BPNN). In terms of lowering energy usage, error rates, and calculation time, the new model outperformed the old one. As a result of [22], a variety of network flow capture formats as well as tools and approaches are presented. Covers the general practice of network security monitoring and incident response and provides lots of background knowledge on network topologies and sensor placement. Common tools are explained, and their usage is demonstrated [23]. present several feature selection algorithms among classification techniques to identify network anomalies and vulnerabilities at various layers. They also cover the assessment of network anomaly detection systems, present different tools and discuss research challenges [24]. Techniques for experimental data analysis, traffic behavior analysis, data collection using sensors and network mapping using python. He also deals with application identification and provides various ways to visualize network data [25].

Describes requirements for a network proxying internet system and explained the structure and functionality of the bro network monitor. Although this paper is more than 20 years old at the time of this writing, it contains fundamental aspects of network security monitoring, and inspired this research project with its philosophy of separating mechanism from policy [26]. to reduce the 41 features widely adopted from the KDD dataset, to only 16 features, while still achieving similar detection results as with the full feature set. They used several filter algorithms including Weight by Maximum Relevance (WMR), Stepwise Regression and Stability Selection. For validation the Bayes Classifier was used, besides Support Vector Machines (SVM) [27]. This research paper served as a motivation for questioning the need for overly complex extracted features and served as a hint to conduct experiments with a more basic feature set.

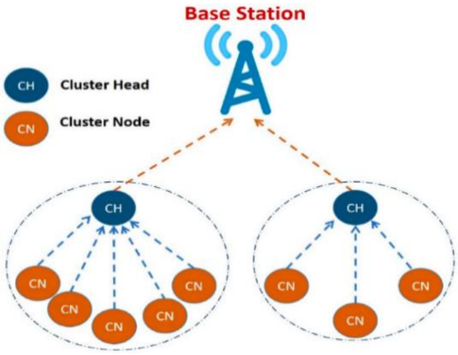

Figure 1. The basic schema of base station with two-cluster head and several cluster nodes [28]

The packet extraction tool for large volume network traces and compared the performance to existing solutions. Unfortunately, while their implementation could have been of great interest to the research community, they do not seem to have released it. The fact that their results could therefore not be evaluated, and that future research will need to continue with inefficient tooling, greatly encouraged me to publish my whole tool chain, in order to assist future researchers and allow independent verification of my results [29]. the analyzed the government of the sculpture for traffic flow testing, provided an overview and comparison of common tools and capture formats. It served as a useful introduction to flow based collection methodology [30].

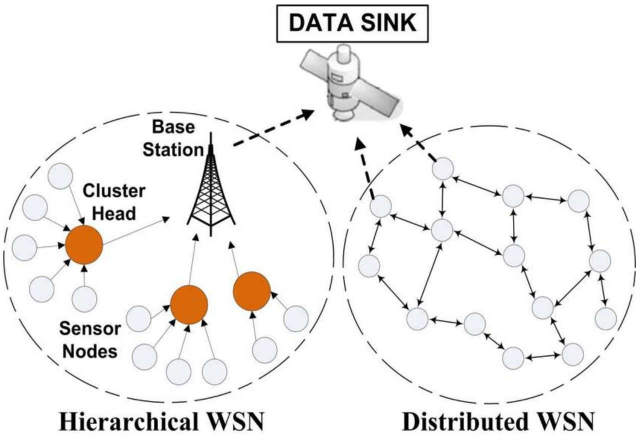

Figure 2. Conceptual model comparison between Hierarchical WSN and Distributed WSN [31]

DL is based on supervised and unsupervised learning methods (ANNs) that are likely to learn hierarchies' embodiments of deep technologies in a supervised or unsupervised manner. Multi-layered processing architectures comprise many different types of DL architectures. For each layer, the information from its input layer can develop non-linear responses. Human mechanisms imitate DL's functionality. Materials used to process signals, such as the brain and other neural structures. Like other types of generic logistic regression, DL architecture has seen an increase in interest in the last few years. DL Architectures consider these techniques to be shallow variants. In 2006, the number of ANNs grew significantly, but the number of DNNs grew significantly over the preceding decades, beginning when it was revealed that there were deep ideological networks in existence. This technology's most recent peak potency has been repeatedly confirmed. Natural language translation and image recognition are two of the most common applications of AI in other industries.

Another factor that contributed to collinearity was the small size of the training data. When FNNs first came on the scene, it was illegal to use their computing power to perform deeper exploration that would lead to new discoveries. Hardware advancements in gpus (GPUs) and broad sense accelerators for hardware have overcome these limitations in coding. Advances in deep network simulation algorithms, as well as in the design levels and areas of DL architectural style depth efficacy, have helped to improve DL architecture depth. The Modulus can learn modified version in DL architectures, compared to conventional ANNs. To begin with. Each layer includes a set of features that can be trained based on the output of the previous layer. To train, each layer encompasses a series of features. The outcomes of the original image were the primary concern. More complex attributes are seen as they double the and multiply in the innermost sphere. Prior to layering, combine features. This is aided by a user-friendly UI. For example, the raw image for portraits can be represented as a vector for a face's description model. Pixels are fed into a model in the input layer. For example, the piece of the edges characterizes cream-based lines, which can be used to classify the first obfuscated layer (the nose, eyes, etc.), which utilizes all the previous qualities to create a face. This is a good example of how each obscured layer can be understood from its predecessor. It's not clear why DL techniques outperform their shallower counterparts, but empirical development analyses have identified improvements in DL models. As far as I know, there's no certainty about it.

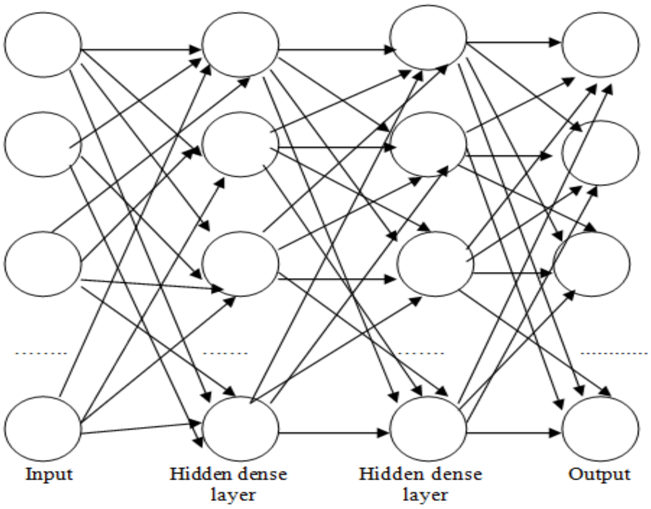

Figure 3. The overall mechanism of deep learning

3. Methodology

One or more physical characteristics are often assessed over a vast region using wireless sensor networks (WSN). A WSN consists of a large number of tiny nodes (sensors). These sensors collect data on environmental factors such as temperature, altitude, humidity, air quality, and more. The monitoring of natural disasters including floods, earthquakes, volcanic eruptions, and other geological catastrophes is one of their many applications. Robotics, chemical, and medical industries are among the other disciplines in which they are applied. Altitude, pressure, humidity, and natural disasters are some of the most prominent WSN applications in the mountains. It is believed that each sensor is a simple screen with a limited power supply and memory, and that it also has a mechanism for sending and receiving data to other nodes, as well as a component for measuring the parameters of the region being monitored. Almost all WSN applications depend on knowing exactly in which the devices are in order to function properly. In fact, the sensors' data is completely meaningless without knowing where they are located. Certain nodes' precise locations may be known in advance in many situations. The remainder of the network's design might be randomly generated and ad-hoc IOT devices in order to reduce the bandwidth required to run the App.

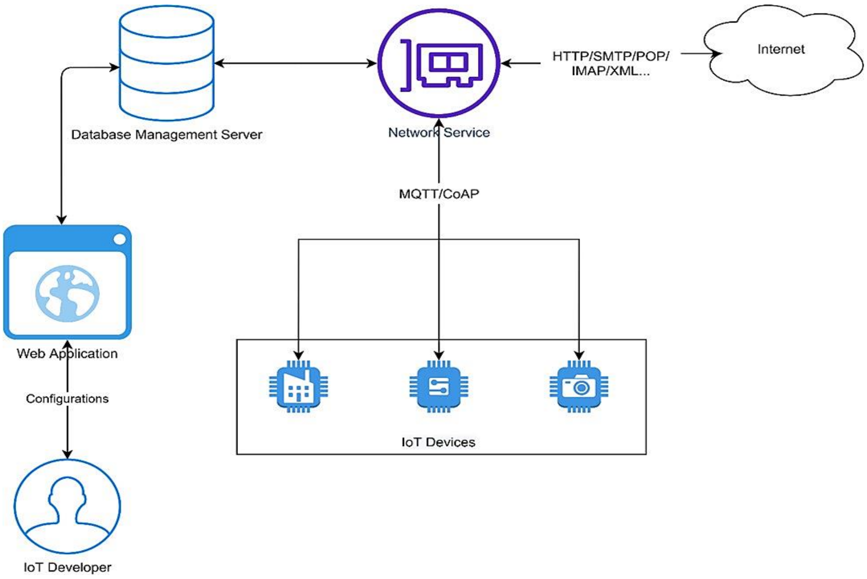

Figure 4. Hierarchy of the proposed system

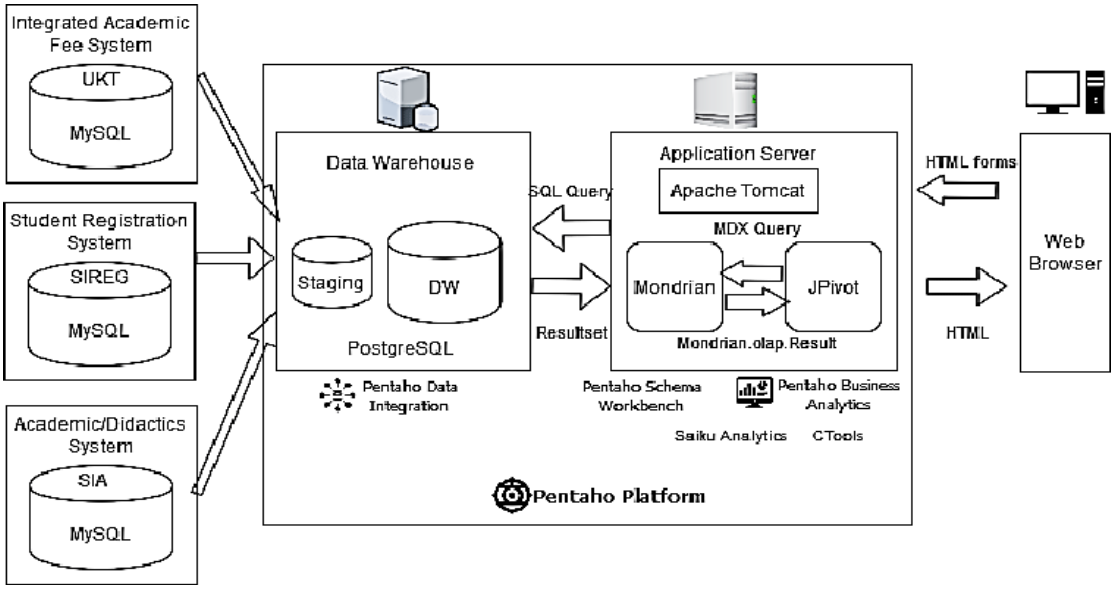

Figure 5. Shapes of an App in the planned structure

We distinguish WSNs from other conventional or wired even wireless networks through sensor based interaction with the environment. WSNs typically possess little (or sometimes no) infrastructure. They consist of a number of sensor nodes which can range from few tens to thousands. These sensors work together to monitor and measure a specific region to obtain information about the environment. In most cases, we are interested in the usage of inexpensive sensors, which intrinsically have limited processing components. This chapter focuses on classification and evaluation of the approaches proposed in the literature for the localization processes for proxying internet system within wireless sensor network. They can be classified in different categories based on various criteria. In the thesis, we consider the problem as distributed systems problem. We also assume the direct connection may not be established across the whole network. Thus, one of the most significant categorizations regarding hardware limitation.

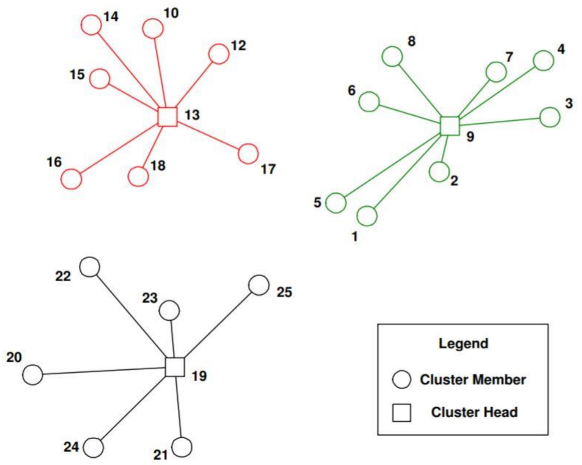

Figure 6. Topology of wireless sensor network after organization into cluster

4. Results

The study of WSN networks and application-level data for a variety of real-time proxy systems. To add to that, prior work on the application-level data only compared a 2-node clustering technique, but we compare and evaluate the accuracy of a 10-node WSNs with clusters. In addition, the study focused on data from the application layer. In spite of this, the data was obtained from an open-source repository and contained a synthetic data set. Our data is derived from an expansive repository for wireless sensor p2p devices and is not synthesized in any way. To further our investigation, we have analyzed the execution times of each method, and we found that our own program required the least time to execute. Our literature research stated that in sensor networks, it was challenging to come up with calculations that could handle large datasets. a large dataset with increasingly precise measurements can be handled by a large number of calculations. There is a 98.68 percent accuracy in wireless sensor computation and the shortest execution time since it operates on several categories but doesn't have any categorization of intermediates in real-time, but rather classifies the "Worms" in a sensor network. A 99.21 percent success rate was achieved in the research using random clusters for intrusion detection and classification on a device system with practically low execution time. For the first time, we're able to accurately detect and characterize real-time proxy kinds and intrusions in sensor-based networks by comparing our results to those of previous studies.

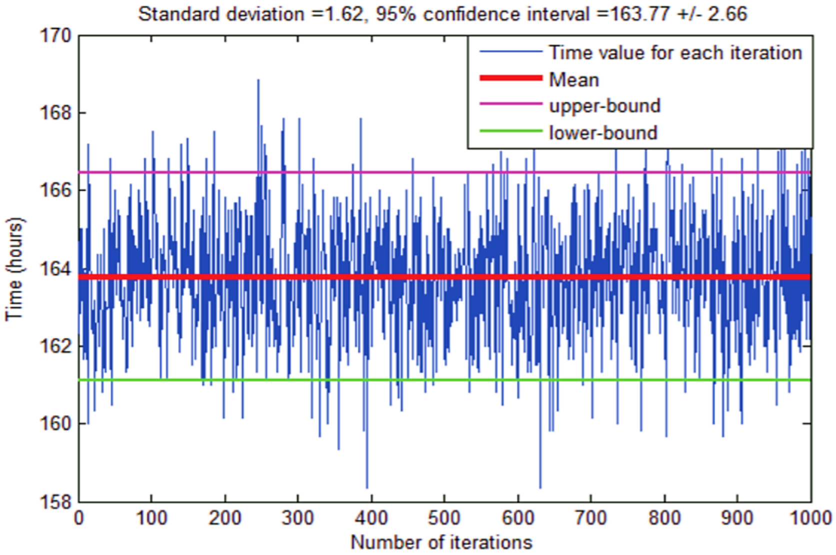

Figure 7. Conveyance plot of the recreation time in the simulation for proxying internet

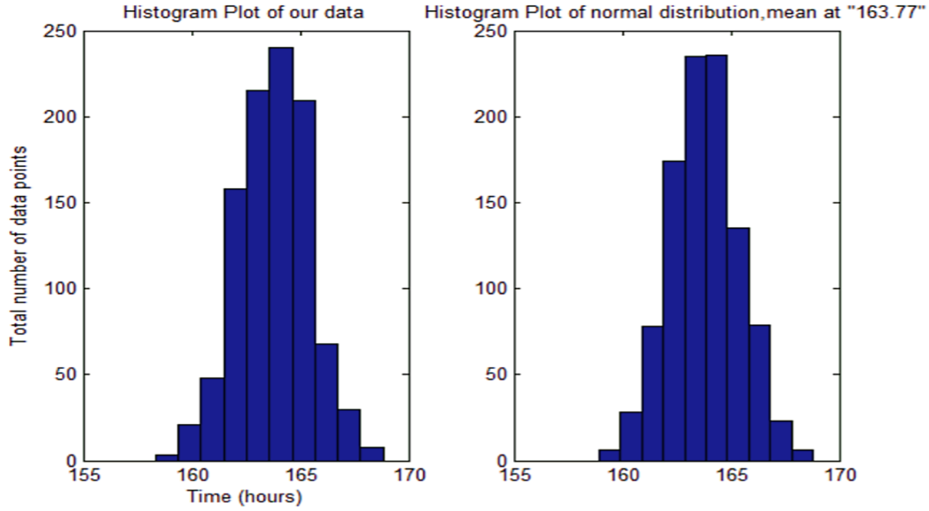

Figure 8. Histogram plot of the reproduction time contrasted with the ordinary conveyance for data points in the WSN

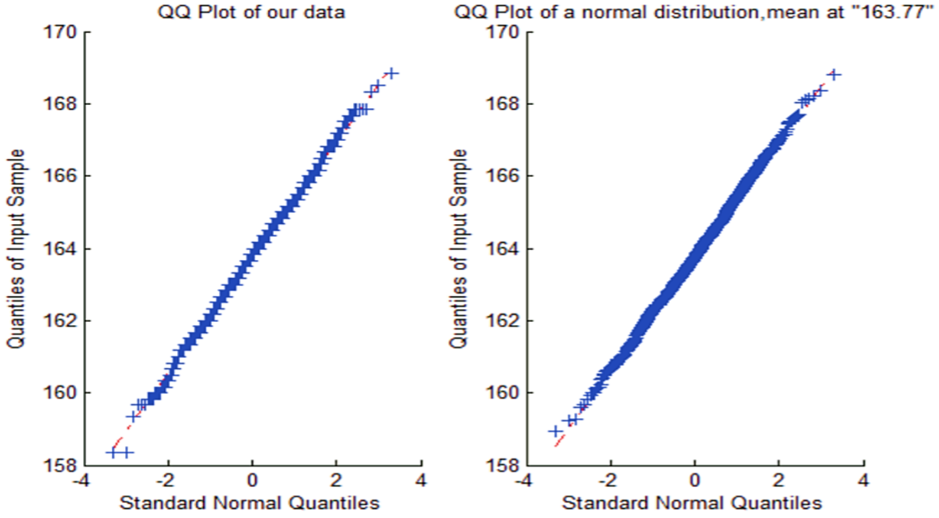

Figure 9. Standard normal quantiles represented in the simulation with time in contrast with the normal distribution

Table 1. comparison between technique

ARTICLE	TECHNIQUE	ACCURACY
[32]	S.V.M	89.97%
[33-37]	C.N.N	96.73%
Proposed	D.N.N	98.68%

5. Conclusion

All WSN intrusions were detected inside clusters and nodes throughout the experiments conducted as part of this analysis. Nodes will be encoded by creating new columns for each original entry and deleting the old columns from the dataset using dummy variables. Boolean values are represented numerically, with a 0 designating false and a 1 indicating true. After more than seven hours of hanging at the multiple regression decoding of the Results columns from Tuesday-WorkingHours-11/DNS labeled.csv, the first run of experiment 1 was ended after 12 hours. The random sample was decreased from 1.0 to 0.5 in order to minimize the number of data that needed to be evaluated. In other words, only half of all the accessible data is used. Conversely, the subsequent run was aborted after eight hours since it failed to reach its destination in a fair length of time. Only 20 percent of the data was used in the third run and the experiment took 29 hours to finish.

WSN will see additional development in the future, with the goal of enhancing unit test coverage and introducing more benchmarks for performance-critical activities. In addition, the WSN network's output will be compared to that of other instruments to ensure that no data is overlooked or misconstrued. Clusters will be enhanced in the future, for example, by adding support for extracted features that have been shown to be useful in other scholarly papers. WSN should also be utilized for experiments with other datasets, to investigate its potential in providing the necessary intelligence for accurate network data predictions Encoding of the feature vectors might be done as part of the WSN framework, which would greatly speed up processing when compared to doing it in a programming language. There will also be an interface for adding new application layer encoders that need stream reassembly.

References

[1] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, “Intrusion prevention framework for secure routing in wsn-based mobile internet of things,” IEEE Access, vol. 7, pp. 185 496–185 505, 2019.

[2] O. B. Mora-Sanchez, E. Lopez-Neri, E. J. Cedillo-Elias, E. Aceves-Martinez, and V. M. Larios, “Validation of IoT Infrastructure for the Construction of Smart Cities Solutions on Living Lab Platform,” IEEE Transactions on Engineering Management, vol. 68, no. 3, pp. 899–908, Jun. 2021.

[3] S. K. Swain and P. K. Nanda, “Priority based adaptive rate control in wireless sensor networks: A difference of differential approach,” IEEE Access, vol. 7, pp. 112 435–112 447, 2019.

[4] J. Li, Z. Xing, W. Zhang, Y. Lin, and F. Shu, “Vehicle tracking in wireless sensor networks via deep reinforcement learning,” IEEE Sensors Letters, vol. 4, no. 3, pp. 1–4, 2020.

[5] M. Shobana and S. Poonkuzhali, “A novel approach to detect IOT malware by system calls using deep learning techniques,” in 2020 International Conference on Innovative Trends in Information Technology (ICITIIT). IEEE, pp. 1–5, 2020.

[6] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, “Machine learning for resource management in cellular and IOT networks: Potentials, current solutions, and open challenges,” IEEE Communications Surveys & Tutorials, 2020.

[7] S. Yao, Y. Zhao, A. Zhang, S. Hu, H. Shao, C. Zhang, L. Su, and T. Abdelzaher, “Deep learning for the internet of things,” Computer, vol. 51, no. 5, pp. 32–41, 2018.

[8] Y. Choi, M. El-Khamy, and J. Lee, “Universal deep neural network compression,” IEEE Journal of Selected Topics in Signal Processing, 2020.

[9] S. Otoum, B. Kantarci, and H. T. Mouftah, “On the feasibility of deep learning in sensor network intrusion detection,” IEEE Networking Letters, vol. 1, no. 2, pp. 68–71, 2019.

[10] W. Lee, M. Kim, and D.-H. Cho, “Deep cooperative sensing: Cooperative spectrum sensing based on convolutional neural networks,” IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 3005–3009, 2019.

[11] A. Singh, S. Rathkanthiwar, and S. Kakde, “Leach based-energy efficient routing protocol for wireless sensor networks,” in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 4654–4658, 2016.

[12] M. M. Rashid and N. A. S. Al-Jamali, “Modified w-leach protocol in wireless sensor network,” Journal of Engineering, vol. 25, no. 3, pp. 68–80, 2019.

[13] J. Guo, C.-K. Wen, S. Jin, and G. Y. Li, “Convolutional neural network based multiple-rate compressive sensing for massive mimo csi feedback: Design, simulation, and analysis,” IEEE Transactions on Wireless Communications, 2020.

[14] A. Mukherjee, P. Goswami, L. Yang, S. K. Sah Tyagi, U. C. Samal, and S. K. Mohapatra, “Deep neural network-based clustering technique for secure IoT,” Neural Computing and Applications, vol. 32, no. 20, pp. 16109–16117, Feb. 2020.

[15] H. Tao, S. Q. Salih, M. K. Saggi, E. Dodangeh, C. Voyant, N. Al-Ansari, Z. M. Yaseen, and S. Shahid, “A Newly Developed Integrative Bio-Inspired Artificial Intelligence Model for Wind Speed Prediction,” IEEE Access, vol. 8, pp. 83347–83358, 2020.

[16] H. R. Abdulshaheed, Z. T. Yaseen, A. M. Salman, and I. Al-Barazanchi, “A survey on the use of WiMAX and Wi-Fi on Vehicular Ad-Hoc Networks (VANETs),” IOP Conf. Ser. Mater. Sci. Eng., vol. 870, no. 1, 2020, doi: 10.1088/1757-899X/870/1/012122.

[17] A. Belmonte-Hernández, G. Hernández-Peñaloza, D. M. Gutiérrez, and F. Álvarez, “Recurrent model for wireless indoor tracking and positioning recovering using generative networks,” IEEE Sensors Journal, 2019.

[18] R. Yang, L. Feng, H. Wang, J. Yao, and S. Luo, “Parallel recurrent convolutional neural networks-based music genre classification method for mobile devices,” IEEE Access, vol. 8, pp. 19 629–19 637, 2020.

[19] X. Zhang, Y. Dong, L. Wen, F. Lu, and W. Li, “Remaining useful life estimation based on a new convolutional and recurrent neural network,” in 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE). IEEE, pp. 317–322 , 2019.

[20] M. Farsi, M. Badawy, M. Moustafa, H. A. Ali, and Y. Abdulazeem, “A congestion-aware clustering and routing (ccr) protocol for mitigating congestion in wsn,” IEEE Access, vol. 7, pp. 105 402–105 419, 2019.

[21] S. Q. Salih, A. R. A. Alsewari, and Z. M. Yaseen, “Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization,” 2019, doi: 10.1145/3316615.3316643.

[22] S. Balakrishna, M. Thirumaran, V. K. Solanki, IOT sensor data integration in healthcare using semantics and machine learning approaches, Springer, pp. 275–300, 2020.

[23] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical IOT systems: A blockchain-based approach, IEEE Network vol. 33, no. 5, 27–33, 2019.

[24] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, “Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices,” IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9603–9610, Jun. 2021.

[25] Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, An IOT-cloud based wear- able ecg monitoring system for smart healthcare, Journal of medical sys- tems vol. 40, no. 12 , 286, 2016.

[26] S. S. Oleiwi, G. N. Mohammed, and I. Al-barazanchi, “Mitigation of packet loss with end-to-end delay in wireless body area network applications,” Int. J. Electr. Comput. Eng., vol. 12, no. 1, pp. 460–470, 2022, doi: 10.11591/ijece.v12i1.pp460-470.

[27] L. Zhou, Z. Qiu, and Y. He, “Application of WeChat Mini-Program and Wi-Fi SoC in Agricultural IoT: A Low-Cost Greenhouse Monitoring System,” Transactions of the ASABE, vol. 63, no. 2, pp. 325–337, 2020.

[28] F. Zantalis, G. Koulouras, S. Karabetsos, D. Kandris, A review of machine learning and IOT in smart transportation, Future Internet., vol. 11, no. 4, p.94, 2019.

[29] D. Rahbari, M. Nickray, Low-latency and energy-efficient scheduling in fog-based IOT applications, Turkish Journal of Electrical Engineering Computer Sciences., vol. 27, no. 2, pp. 1406–1427, Mar. 2019.

[30] U. Beyaztas, S. Q. Salih, K. W. Chau, N. Al-Ansari, and Z. M. Yaseen, “Construction of functional data analysis modeling strategy for global solar radiation prediction: application of cross-station paradigm,” Eng. Appl. Comput. Fluid Mech., vol. 13, no. 1, pp. 1165–1181, 2019, doi: 10.1080/19942060.2019.1676314.

[31] M.-D. Gonza´lez-Zamar, E. Abad-Segura, E. Va´zquez-Cano, E. Lo´pez- Meneses, IOT technology applications-based smart cities: Research analy- sis, Electronics., vol. 9, no. 8, p.1246, 2020.

[32] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. Mohammad Salih, "A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks," Wirel. Pers. Commun., vol. 75, no. 4, pp. 2495–2511, 2014, doi: 10.1007/s11277-013-1479-z.

[33] M. D. Hassan, A. N. Nasret, M. R. Baker, and Z. S. Mahmood, "Enhancement automatic speech recognition by deep neural networks," *Period. Eng. Nat. Sci.*, vol. 9, no. 4, pp. 921–927, 2021, doi: 10.21533/pen.v9i4.2450.

[34] I. Al_barazanchi, Z. A. Jaaz, H. H. Abbas, and H. R. Abdulshaheed, "Practical application of iot and its implications on the existing software," Int. Conf. Electr. Eng. Comput. Sci. Informatics, vol. 2020-Octob, no. October, pp. 10–14, 2020, doi: 10.23919/EECSI50503.2020.9251302.

[35] I. Al Barazanchi, A. Murthy, A. Abdulqadir, A. Rababah, and G. Khader, "Blockchain Technology - Based Solutions for IOT Security," Iraqi J. Comput. Sci. Math., vol. 3, no. 1, pp. 1–12, 2022.

[36] Z. A. Jaaz, I. Y. Khudhair, H. S. Mehdy, and I. Al Barazanchi, "Imparting Full-Duplex Wireless Cellular Communication in 5G Network Using Apache Spark Engine," Int. Conf. Electr. Eng. Comput. Sci. Informatics, vol. 2021-Octob, no. October, pp. 123–129, 2021, doi: 10.23919/EECSI53397.2021.9624283.

[37] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.