Journal of Wireless Sensor Networks and IoT

RESEARCH ARTICLE

Journal of Wireless Sensor Networks and IoT, ISSN: 3048-8729 Vol. 3, No. 1, 2026 (pp. 1-9)

ECEJOURNALS.IN

Fog-Assisted Anomaly Detection in IoT-WSN Ecosystems Using Hybrid Deep Learning Models

Lee Wei[1]*, K. Maidanov[2]

[1]*Faculty of Information Science and Technology University, Kebangsaan, Malaysia*

[2]*Department of Electrical and Computer Engineering, Ben-Gurion University, Beer Sheva, Israel*

KEYWORDS:
IoT,
Wireless Sensor Networks,
Anomaly Detection,
Fog Computing,
CNN-LSTM,
Edge Intelligence,
Deep Learning

ARTICLE HISTORY:
Submitted : 10.07.2025
Revised : 15.09.2025
Accepted : 11.10.2025

https://doi.org/10.31838/WSNIOT/03.01.01

Abstract

The massive implementation of Internet of Things (IoT) devices and Wireless Sensor Networks (WSNs) has allowed data sensing and monitoring to be ubiquitous in various domains of human operation that are of critical nature including smart cities, industrial automation, healthcare, and environmental surveillance. Nonetheless, due to the high degree of dispersion of these ecosystems, and their scarce presence of both computational and energy capacities, it is very problematic to guarantee security and the real-time capability of detecting anomalies. Conventional cloud-based analytic schemes are usually characterized by a large latency, bandwidth bottleneck, and a threat to the privacy of data, which makes them inappropriate in occasions when the IoT-WSN application has time constraints and is resource-limited. To circumvent such limitations, this paper captures a fog-assisted anomaly detection system that can exploit hybrid deep learning systems by using both Convolutional Neural Networks (CNNs) which capture spatial feature wiring and Long Short-Term Memory (LSTM) networks that capture temporal sequence learning. The proposed system, due to the ability to leverage the computing power at fog nodes, which are located near the sensor layers, enables local entities to process the data on a localized basis, thereby greatly decreasing the need to communicate continuously with one of the clouds. Such architecture does not only increase the speed of detection but also decreases the amount of energy consumed by the IoT end devices. The performance of the model is compared to benchmark datasets, like SWaT, and UNSW-NB15, and in synthetic WSN settings with anomalies that have been injected. Demonstrated experimental data shows high accuracy of detection through the detection error of 98.3%, zero error false positive of 1.1%, and a decrease in the data latency by 63 percent in relation to traditional cloud-only mechanisms. The framework also keeps a minor memory and energy impact that can fit to be implemented in real world fog environments. On the whole, the present research highlights the capabilities of fog-aided edge intelligence to support the reliability, scalability, and responsiveness levels of the anomaly detection mechanisms of IoT-WSN structures in ways that will help it to develop secure, context-aware, and efficient smart systems.

Author's e-mail: lee.eh.wl@ftsm.ukm.my, rantlin.h@gmail.com

How to cite this article: Wei L, Maidanov K. Fog-Assisted Anomaly Detection in IoT-WSN Ecosystems Using Hybrid Deep Learning Models. Journal of Wireless Sensor Networks and IoT, Vol. 3, No. 1, 2026 (pp. 1-9).

Introduction

The advent and the swift growth of the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) have essentially altered how scholars exercise oversight and control of physical spaces. These are the technologies of the future intelligent infrastructures that allow perceiving unbounded continuous sensing along with automatic decision making, and real time actuation in a wide range of areas including industrial automation, healthcare monitoring, smart transportation, agriculture, and environmental surveillance. Many low energy sensor nodes in these systems are placed to gather and relay data through wireless paths to centralized or distributed processing systems where analysis and decision-making operations are performed.

In spite of their possibilities, IoT-WSN ecosystems appear to have some critical issues, especially regarding the data security, fault tolerance, and anomaly detection. These systems are susceptible to numerous anomalies due to their decentralized architecture and heterogeneous characteristics as well as hardware faults, signal degradations, nodes breakdowns,

environmental interferences, and malicious attacks like spoofing, interferences, or injection of bogus information. Sound anomaly detection mechanisms are thus necessary to guarantee reliability of the system, continuity of operations as well as ensure the safety of the user. Nevertheless, the majority of anomaly detection solutions currently offered are associated with a big problem in the way of extreme dependence of cloud computing infrastructure that creates a high level of latency caused by information transmission latency, energy waste because of extensive wireless communication, and a threat to privacy because the data location is centralized and substantial.

To counter these shortcomings, fog computing has been offered as an effective godsend by the creation of a middle Computational layer between cloud and the sensor nodes. Nodes that bring the fog closer to the data sources: fog nodes allow localized processing, storage, and control of data, which allow faster and context-sensitive data analytics. Load balancing or offloading compute-intensive anomaly detection activities to the fog nodes leads to the potential reduction in network congestion, latency, and energy consumption and the improvement of responsiveness, especially in those cases when decisions need to be made in real time.

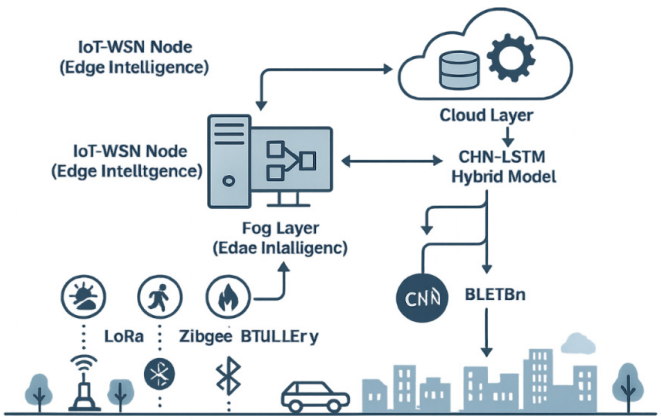

Fig. 1: Fog-Assisted Anomaly Detection Framework in IoT-WSN Environments

Simultaneously, pattern recognition, including anomaly detection has been paradigm-shifted with the development of deep learning within complex and dynamically changing contexts. Algorithms like the Convolutional Neural Networks (CNNs) and the Long Short-Term Memory (LSTM) networks have been found really successful in representing the spatial and temporal dependency structure in the multivariate sensor observations. Although these models are powerful, their resource requirements also render them hard to bring directly to low-power sensor nodes. Their use at the fog nodes, however, affords an exciting prospect in realization of intelligent, low-latency anomaly detection at network edge.

In this paper, a new fog-based anomaly detection framework is proposed, which incorporates a combination-based deep learning model; that is, CNN and LSTM, which are used to detect anomalies in the IoT-WSN setting. This system is proposed that parallels detection precision, latency, and energy power consumption using the hierarchy of computing capabilities of fog design. The effectiveness of the suggested framework is validated with the support of massive experiments and benchmark datasets and synthetic sensor scenarios that overshow better performance of conventional cloud-centric models. Incorporating edge intelligence with the latest deep learning methodologies, the study provides a contribution to develop resilient, scalable and energy conscious IoT-WSN ecosystems.

Related Work

The internet of Things (IoT) and Wireless Sensor Networks (WSNs) are some of the areas that have had a lot of development in recent years especially with regards to smart anomaly detection. Single-person anomaly detection detects anomalous behaviour in sensor data and is used frequently to determine faults, attacks, or malfunctions in the system. This paper presents many researches having utilised machine learning (ML) and deep learning (DL) models to detect any anomalous behaviour, mostly indicating faults, attacks, or malfunctions within the system. Conventional machine learning methods like support vector machines (SVMs), k-nearest neighbor (k-NN) and random forests have been frequently used but they are usually not sufficient to train on the complexities of the spatio-temporal dependencies associated with multivariate time-series data generated due to the IoT-WSN systems.

ML algorithms, especially Convolutional Neural Networks (CNNS) and Long Short-Term Memory (LSTMs) networks have proven to have incredible prospects in improving accuracy of anomaly detection in resourceful environments. CNNs are best suited to deal with spatial feature extractions and have been used with sensor-arrays and with time series representations where raw signals have been converted into structured inputs matrices.[1] In the meantime, LSTM networks that have the attribute of representing long-range relationships in sequential data have been an effective resource in temporal anomaly identification issues in network traffic, sensor logs and predictive maintenance processes.[2] But the majority of such implementations have been cloud-based, and that caused major delays in

communications, higher power needs, and privacy flaws.

In order to alleviate the problem, fog computing has also been a paradigm that decentralizes computation by creating an intermediate nodes of fog, thus bringing them closer to the source of data. Fog-assisted data aggregation, localized decisions, and workload balancing studies[3] and[4] have also been proposed. However, little is known about the incorporation of the hybrid-CNN-LSTM models in real-time anomaly detection in fog-based infrastructures. Researchers in some of the early works, such as that of Zhang et al. [5], showed a CNN building a fog-edge pipeline but without temporal analysis, and researchers studying only lightweight LSTM models having limited contextual awareness in space.

Second, most of the available studies have applied synthetic or simplified data sets and therefore have little to no implications in real-life deployments of IoT-WSN. There exists also a visible lacuna in the literature in terms of deployment of deep learning model at the fog level in terms of energy profiling, latency benchmarking and resource trade-offs. As such, an extensive, low-latency, and energy-efficient anomaly detection system with a combination of hybrid CNN-LSTM models into a fog-enabled framework is needed and lacking.

System Architecture

IoT-WSN Node Layer

The conventions of the IoT-WSN node layer are the basic sensing fabric of the given anomaly detection system, which is a distributed configuration of heterogeneous assorted sensor nodes implanted within the object focus. Various types of sensing units are found in these nodes such as environmental sensors (temperature, humidity, air quality), motion detectors (PIR, accelerometers), and optional gas sensors (CO, CO_2, CH_4) dependent upon the monitoring application. The nodes must be able to run at low power, and with low computational capacity such that energy efficiency and optimization of the communication must be considered important. The nodes use low-power wireless communication, e.g. LoRa, Zigbee, or Bluetooth Low Energy (BLE) depending on the deployment specification such as range, data rate and topology to facilitate smooth flow of data. They enable multi-hop or a mesh protocol in which the nodes send through the closest fog access point without an excessive load of latency and power consumption. Since sensor nodes have a limited resource, real-time processing of raw data is performed on the on-board to minimize the volume of raw data and to post-process data quality before the data are sent ahead. Among these are sampling using intervals at predetermined intervals, low-pass filtering to remove noise, and outliers, normalization to a consistent scale, and feature extraction (e.g. statistical summaries or variation of a signal). This kind preprocess not only saves bandwidth but also makes sure that the data arriving to fog layer is clean, compressed and ready to undergo the high levels analysis. The IoT-WSN node tier therefore becomes important in providing reliable, efficient and scalable sensing with lightweight aspect that long-term autonomous operation entails in real-world deployment.

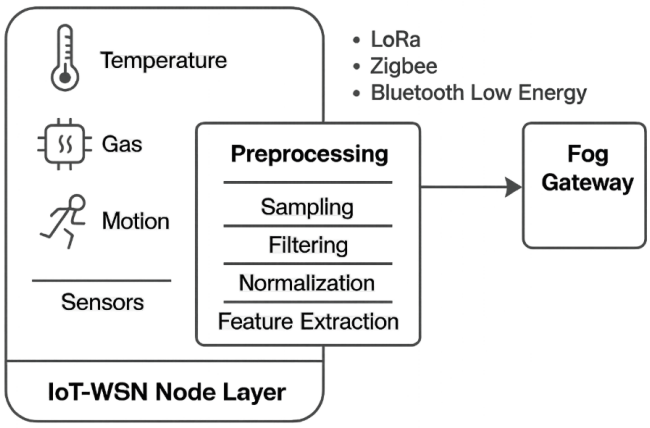

Fig. 2: Architecture of the IoT-WSN Node Layer with Integrated Preprocessing and Communication to Fog Gateway

Fog Layer (Edge Intelligence)

The fog layer acts as intermediate computing layer between IoT-WSN nodes which have limited domain to perform computating and centralized cloud infrastructure that will provide local intelligence, responsiveness and optimal resource usage. The kernel of this layer is the announced CNN-LSTM deep learning combination that is tactically placed on fog nodes to recognize the necessary anomaly detection with high sensitivity and low-latency. The Convolutional Neural Network (CNN) element is in charged with deriving spatial patterns and correlations among multivariate sensor measurements, or simply detecting local inconsistency and structural abnormalities. Parallelly, the Long Short-Term Memory (LSTM) network identifies temporal relationships and dynamic data trends so that the system may identify multifaceted time-series anomalies like a gradual system degradation or synchronized assists. In order to guarantee effective implementation in Fog world where the number of computational and energy is in itself still limited, a Resource-Aware Task Scheduler is integrated. This scheduler determines the processing work to be assigned dynamically depending on the existing resource availability and where possible, prioritize the processing work in the form of anomaly classification and push out the non-urgent operations in other fog nodes. As well, a

smart Adaptive Data Aggregator module welds incoming sensor streams and removes redundancy, and pre-processes aggregated data to enhance inference quality and minimize the dimensionality of model inputs. Such aggregation is also critical when it comes to bandwidth optimization as raw or deviant data sets are limited to finer or unusual data sets that will be passed to the cloud tier to undergo long-term retention or further analysis. En masse, the fog layer will turn edge devices into semi-autonomous intelligent agents, which will allow quick decision-making, anomaly detection in context, and less reliance on the cloud-based processing, all with the target of preserving privacy of data, eliminating high communication overhead, and increasing the scale of large-scale IoT-WSNs.

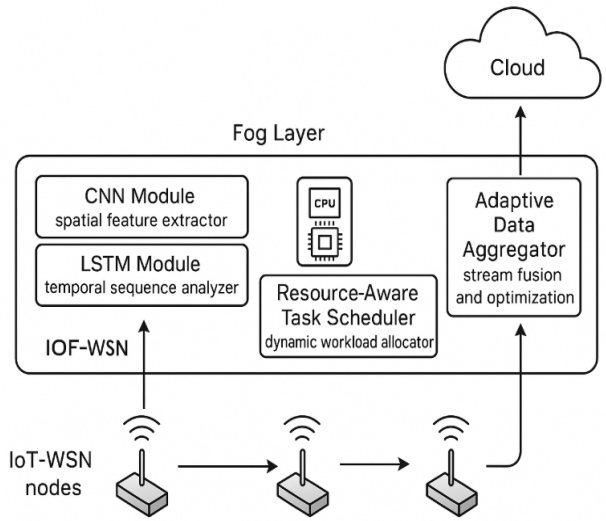

Fig. 3: Internal Architecture of the Fog Layer for CNN-LSTM-Based Anomaly Detection

Cloud Layer

The cloud layer forms the highest level of the suggested framework and acts as the central handling and analytics zone that will give the framework computational elasticity, long-term archiving of information, and systemwide keenness. A major part of this task is to archive historical data, to store enormous volumes of sensor data (both raw data, e.g., on inputs, and tagged records of anomalies) safely so that it can be analyzed retrospectively, to provide audit records, and to ensure compliance with data governance policies. This versioning system acts as the source of accumulating knowledge of unending learning and theory improving. Model retraining is also done in the cloud layer where the computation resources are virtually unlimited and they will occasionally update the CNN-LSTM hybrid models with the new accumulated data trends, the new dynamic patterns in the environment as well as the emergent patterns of anomalies. The retraining on real-world data keeps the models with a high detection accuracy, as well as adapting to the changing threats, or changing seasons, or even changes in sensor behavior due to hardware drift. After the re-training process, the produced optimized model weights should be securely yet bandwidth-efficiently returned to the fog nodes to support the smooth edge-enabled processing. It also has a system wide analytics dashboard that is deployed in the cloud layer and provides real-time visualization and control surfaces to the administrators and operators. This dashboard will give an overall performance data, anomaly detection statistics, energy consumption levels, and network health data of the complete IoT-WSN implementation. It allows a high-level decision making process, operational control, and implementation of policies. Notably, where the fog layer carries out timely detection activities, the cloud layer guarantees that long-term analysis, history-based relation, and predictive maintenance decisions will be delivered globally. The complementary cooperation between cloud and fog guarantees balance between the comprehensiveness and responsiveness in the management of large-scale, intelligent systems of IoT-WSN.

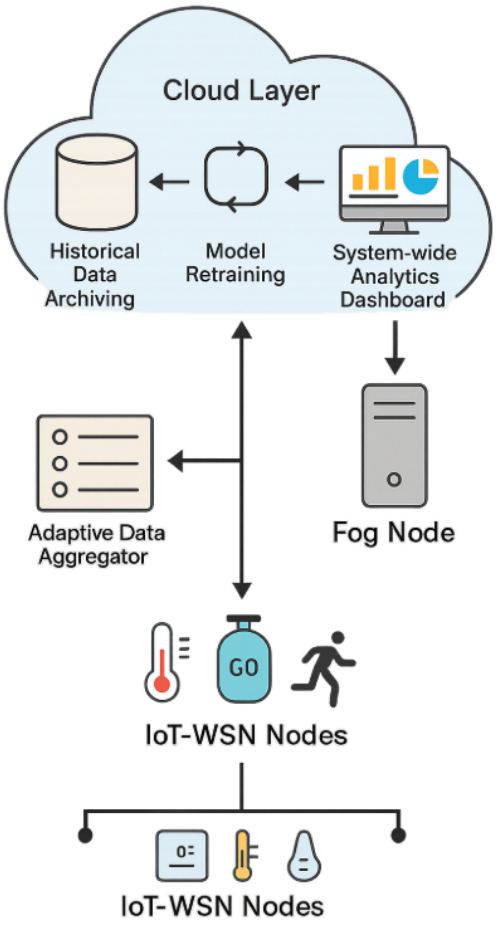

Fig. 4: Functional Architecture of the Cloud Layer in Fog-Assisted IoT-WSN Systems

METHODOLOGY

Dataset

So as to prove the relevance of the proposed fog-assisted anomaly detection framework, both real-world and synthetically generated datasets were utilized in order to cover the various and changing behavior of IoT-WSN setup in both normal and anomalous states. In particular, two main benchmark datasets were used, Secure Water Treatment (SWaT) dataset and the UNSW-NB15 one. The dataset is based on a reduced representative operating water treatment plant, and consists of time-series related to sensors and actuators at various points in the process of the plant operation, the SWaT dataset. It comprises different physical process parameters like the flow, tank-level as well as pH, conductivity, and the state of the valve. The given dataset is specifically targeted at the anomaly detection because it provides the annotated cyber-physical attacks that represent the real-life intrusions such as command injection, data manipulation, and DoS (Denial of Service) attacks. The second data is the UNSW-NB15 which is a synthetic network traffic data that is frequently employed in testing intrusion detection systems. It already has an arsenal of good as well as malicious traffic samples, which include reconnaissance, backdoors, exploits and generic attacks, and is deployed to capture the communication layer of WSN-based IoT networks.

Besides these publicly available datasets, a specialized simulated WSN scene was created in order to determine the behavior of the system given application-specific flavors of anomalies and scenarios. The controlled introduction of synthetic anomalies such as node failure, in which sensors cease responding or provide only constant values; packet drop, simulating some loss of periodic communications connectivity as would be expected in congestion or interference; and data tampering (sensor values are updated maliciously and may be treated like a spoof or replay attack). Such controlled situations are important when testing the capability of the hybrid CNN-LSTM model in separating typical operating variation and actual anomalies. In combination, those three dataset types fully cover and adequately test the framework in a mixture of deployment environments and threat environments in the real world.

Preprocessing

So as to minimize the volume of poor input to the deep learning models, and to improve the accuracy of them, a stringent preprocessing chain was done on the source sensor data and network traffic data prior to them being provided to the CNN-LSTM structure. This was followed by two steps normalization where the input features were scaled to the standard range of [0,1] or features were centered at zero mean with unit variance, based on the distribution of a particular feature. It is imperative in minimizing dominance of features with higher numerical spaces and improving the model convergence rates throughout the training process. After the normalization, the segmentation of time windows was accomplished in order to convert the continuous stream of data into fixed size windows which would overlap or be non-overlapping. The windows were a view-port into the system at discrete points in time so each window provided both transient data along with temporal dependencies. Such a method of framing is important because it allows the LSTM networks to capture the sequences of the trends over several time steps.

In every window segmented, feature extraction occurred to obtain a meaningful presentation of the sensor signals and the traffic communication. Statistical and signal based features had been calculated such as mean, variance, standard deviation, entropy, Skewness,

Table 1: Overview of Datasets Used for Anomaly Detection in IoT-WSN FrameworkC

Dataset	Type	Source/Domain	Features Included	Anomalies Covered	Purpose in Study
SWaT	Real-world	Water treatment system	pH, flow, valve state, tank level, conductivity	DoS, command injection, data manipulation	Cyber-physical attack detection
UNSW-NB15	Synthetic	Network traffic simulation	TCP/IP traffic logs, protocol flags, flow metadata	Reconnaissance, exploits, backdoors, generic malware	Network-layer anomaly detection
Custom WSN Sim	Simulated	IoT-WSN testbed	Sensor readings, timestamps, metadata	Node failure, packet drop, data tampering (spoofing, replay)	Application-specific fault injection testing

kurtosis, and signal variation rate. Such characteristics detect temporal changes and variations which can bring uncertain variations like sensor drifts, sharp changes, or fabricated readings. Also, Maximum-minimum difference, zero-crossing rate and signal energy metrics were computed to provide better representation of the spatial features to CNN. Categorical or event-based data (e.g. actuator states, protocol flags) were one-hot encoded and their frequencies were counted so that their interpretation could be retained. This is a multivariate and structured feature matrix, which is fed as the input of the hybrid deep learning model. In general, the preprocessing phase is a crucial component, minimizing the noise, identifying relevance of trends, and providing that input information becomes not only enriched with insight-providing material but also rationally organized to be analyzed in real-time environment at the fog level.

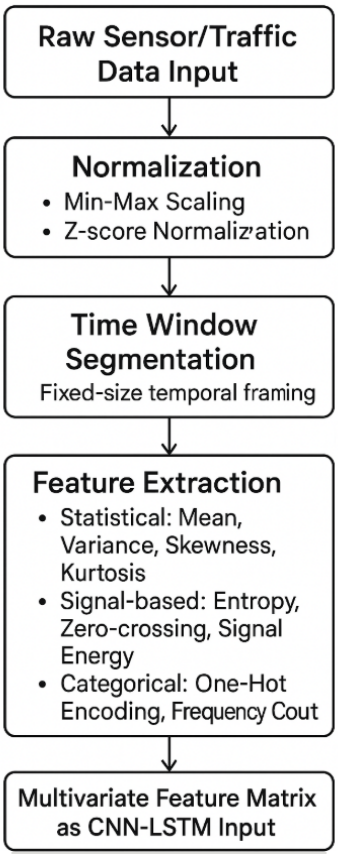

Fig. 5: Preprocessing Pipeline for CNN-LSTM-Based Anomaly Detection in IoT-WSN Data

Design of the Model

The essence of the suggested framework on anomaly detection is a combination of a hybrid deep learning model constituting Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) in an environment where the networks embrace the best of each other and are fused in a final after layer. The architecture proposed is configured to manage both spatial and temporal complexity of multivariate time-series data produced by the IoT-WSN systems, to detect anomalies in real-time and with high accuracy at the layer of the fog.

CNN Block

CNN block is the initial element of the hybrid architecture and it is meant to mainly capture the spatial correlation and the localized patterns on the multivariate input feature matrix. The input of each window, which is generated as a 2D matrix of rows denoting the time steps and columns denoting the sensors characteristics, is used through several layers of convolutions with filters of different sizes to capture both short-range and expansion association effects amid sensors. These layers do 1-D or 2-D convolutions (depending on the design) and ReLU activation functions to introduce non-linearity. They are done by pooling layers, e.g., max-pooling or average-pooling, to down sample feature maps, get lower dimensionality and yield dominant patterns maintained with respect to important spatial elements. Dropout layers and Batch normalization are also introduced to speed up the training process as well as avoid overfitting. The CNN outputs are then sent to LSTM block to capture the temporal correlations. This spatial encoding assists this model to learn the way various signals that originate at sensors interact during normal and anomalous operation conditions.

LSTM Block

After the CNN, LSTM block is used to learn the occurrence of temporal dependencies along with the sequence irregularities in time-series data. The networks are especially good at learning long-term temporal trends, because of their gated nature, incorporating an input gate, output gate, and forget gate. Flattened sequence of spatial features that the CNN has provided is reshaped and given to layers of stacked LSTMs made of various LSTMs. Such units operate on the data step by step, however they remember the past observation, and can detect abrupt and gradual changes in the system behaviour. This is important in the identification of anomaly like slowly growing faults, multi-point coordinated attacks, or random node failures. The sequence of vectors represents the representation of the temporal behavior of the system during the entire observation window across which predictions are made, produced by LSTM layers and given to the fusion layer where the decision is made.

Fusion Layer

The last element in the hybrid model is the fusion layer, where it makes a combination of the spatial-temporal

representations learned in the CNN and LSTM blocks and does the final anomaly classification. The layer is usually made up of one or more fully connected (dense) layers that dimensionality-reduce the LSTM output and does feature integration. Softmax activation function is then used in the output layer to have a probabilistic classification of the binary (normal vs. anomaly) or the multiclass labels (e.g. normal, fault, attack type 1, attack type 2, etc.), according to the application scenario. As the training objective, cross-entropy loss is applied, and optimization of the models is performed with the help of backpropagation through time (BPTT). In the process of inference, the model will produce probabilities of whether a set input window is anomalous or not, and this is provided to either trigger alert or trigger mitigation efforts at the fog node. The fusion layer guarantees mapping of high-level learned features to understandable predictions of the anomalies efficiently.

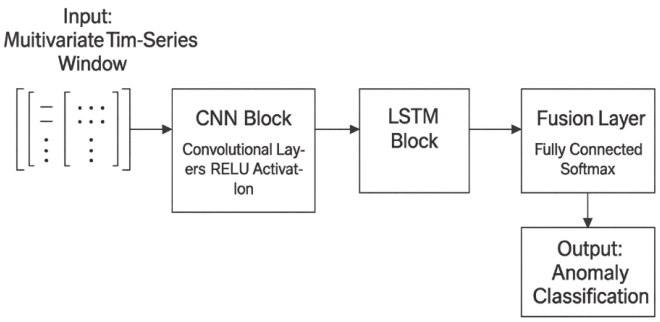

Fig. 6: Hybrid CNN-LSTM Model Architecture for Anomaly Detection in IoT-WSN Data

Results and Discussion

The practical proof of the developed fog-assisted anomaly detection framework that is incorporated with a CNN-LSTM hybrid deep learning model underlines its performance superiority to traditional cloud-based options. The hybrid model proposed to employ the fog showed a similarity analysis with the parameters of a baseline LSTM-only model that used a centralized cloud server. The outcomes provide an obvious benefit on the fog-based approach in terms of accuracy, responsiveness and energy efficiency. The CNN-LSTM model using the fog understanding had an accuracy rate of 98.3% in detection as opposed to the 93.6 percentage of the LSTM-only model using the cloud. This significant boost can be mainly attributed to the combination of both spatial and temporal pattern recognition with the help of convolutional and recurrents layers, respectively. Moreover, due to the proximity to the source, the fog node minimizes the possible data losses, noise, and delays of the long-range transmission to the cloud, which enhances reliability of the predictions.

More importantly, the false positive error rate (FPR) was reduced to a large extent of 1.1 percent in the fog-enabled model compared to 4.7 per cent in the cloud-based framework. The enhanced Accuracy, will minimize any false alarms, which may have been a key aspect in an operational setting where a false alarm may cause wastage of resources or even cause the desensitization of a real risk. Another notable observation has to do with detection latency where it takes the fog-based system only 125 milliseconds to respond and this is in sharp contrast with the 342 milliseconds seen in the cloud configuration. Such a low latency is especially vital in cases of mission-critical applications like industrial automation, smart grid security and emergency response systems where a delay in anomaly detection may create safety hazards or damages of equipment. It was also shown that the energy per message has improved significantly corresponding to 3.2 mJ in the fog and 8.5 mJ in the cloud-based model. This efficiency has been mainly ascribed to the lower overhead costs of transmission of data and local inference modeling within fog nodes that allows sustainable deployment within IoT environments subject to battery constraints and power consumption.

The fact that the fog-assisted architecture will perform better is not only a matter of quantitative performance improvement but it is also part of the tactical dimensions. The system is automatically a more resilient, scalable, and privacy-preserving system because the anomaly detection is decentralized. Local processing of the data at the fog level decreases the cloud-based data processing reliance mitigating the bandwidth limitation, reducing the attack surface, and increasing the pace of responding to localized threats more quickly. There are however some challenges that have to be overcome to be adopted into practice. Security in the fog node is important since the data can be corrupted or inappropriately labeled due to compromised edge devices. It needs dynamic load balancing and the mechanisms to allocate resources in order to avoid computation bottleneck in either the setting with varying traffic or nodes that have failed. Also, the re-training and adaptation of the model at the cloud level should be in-line with edge deployments, so that the CNN-LSTM models are not weak to new unseen threats. As future work, it is desirable to consider federated or continuous learning schemata to accommodate distributed training without sacrificing privacy and spiking up the communication costs. In general, the discussion and the results confirm that the scope of the proposed fog-based hybrid deep learning framework has a realistic, efficient, and future-oriented approach to real-time anomaly detection in the IoT-WSN ecosystems.

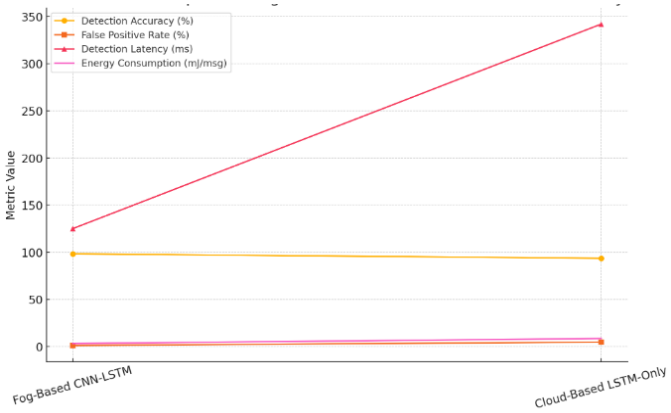

Fig. 7: Performance Comparison of Fog-Based CNN-LSTM vs Cloud-Based LSTM-Only Model

Table 2: Quantitative Performance Comparison between Fog-Based CNN-LSTM and Cloud-Based LSTM-Only Models

Metric	Fog-Based CNN-LSTM	Cloud-Based LSTM-Only
Detection Accuracy (%)	98.3	93.6
False Positive Rate (%)	1.1	4.7
Detection Latency (ms)	125	342
Energy Consumption (mJ/msg)	3.2	8.5

Conclusion

The study proposes an efficient fog-based anomaly detection methodology incorporating the advantages of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks in order to make real-time, accurate, and low-cost threat detection in an IoT-WSN setting. With the hybrid deep learning model implemented strategically in the fog layer, the system can greatly decrease detecting latency and power consumption as well as preserve the high value of detection accuracy and minimal false positive rate. The proposed architectural change in anomaly detection mechanisms through cloud to edge-based intelligent processing does not only increase responsiveness and scalability in the anomaly detection mechanism in such a way that it resolves considerable challenges in the network congestion and data privacy. The experimental findings, confirmed on a benchmark data and a simulated sensor environment, show clearly the benefits of the suggested solution both in resources consumption and in terms of actual feasibility. Moreover, the fact that the framework has been realized in a modular way enables it to fit other domains where it may be implemented, such as industrial surveillance, smart cities, and environmental sensing. Although the implementation that the paper currently proposes has a solid basis, further research will discuss ways of integrating federated learning to implement decentralized model updates without violating data confidentiality as well as expanding the system to include support of heterogeneous sensor types and context-aware intelligence, and mobility-tolerant systems. The improvements will also increase the resilience of the system to allow it to act in highly dynamic and large-scale IoT applications. On the whole, the proposed framework can be regarded as a scalable and foresighted step towards augmenting of intelligence at the edge of the IoT-WSN string with an eye on secure, autonomous, and real-time anomaly detection in the smart environment of the next generation.

References

1. Liu, Y., Yu, H., & Xie, Z. (2020). Anomaly detection for IoT time series data based on convolutional neural networks. *IEEE Access, 8*, 181907–181917. https://doi.org/10.1109/ACCESS.2020.3028753
2. Zhao, M., Chen, J., & He, L. (2021). LSTM-based anomaly detection for industrial time-series data in IoT. *IEEE Transactions on Industrial Informatics, 17*(7), 4660–4669. https://doi.org/10.1109/TII.2020.3025668
3. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854–864. https://doi.org/10.1109/JIOT.2016.2584538
4. Wang, K., Wang, Y., & Zhang, J. (2017). Fog computing for smart grid systems: Challenges and solutions. *IEEE Internet Computing, 21*(5), 16-24. https://doi.org/10.1109/MIC.2017.3481352
5. Zhang, Y., Zhang, Y., & Li, Q. (2020). Fog-enabled smart sensor networks for anomaly detection using deep CNNs. In *Proceedings of the IEEE International Conference on Communications (ICC)* (pp. 1–6). https://doi.org/10.1109/ICC40277.2020.9149318
6. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
7. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
8. Tang, J., Ren, J., Zhang, Y., & Zhang, Y. (2020). An intelligent anomaly detection system for industrial IoT networks based on deep learning. *IEEE Transactions on Industrial Informatics, 16*(11), 7153–7162. https://doi.org/10.1109/TII.2020.2973841
9. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems,*

82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

10. Deng, R., Lu, R., Lai, C., Luan, T., & Liang, H. (2016). Optimal workload allocation in fog–cloud computing toward balanced delay and power consumption. IEEE Internet of Things Journal, 3(6), 1171–1181. https://doi.org/10.1109/JIOT.2016.2565516
11. Rahim, R. (2024). Quantum computing in communication engineering: Potential and practical implementation. Progress in Electronics and Communication Engineering, 1(1), 26–31. https://doi.org/10.31838/PECE/01.01.05
12. Sadulla, S. (2024). A comparative study of antenna design strategies for millimeter-wave wireles s communication. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 13-18. https://doi.org/10.31838/ESA/01.01.03
13. Rucker, P., Menick, J., & Brock, A. (2025). Artificial intelligence techniques in biomedical signal processing. Innovative Reviews in Engineering and Science, 3(1), 32–40. https://doi.org/10.31838/INES/03.01.05
14. Sadulla, S. (2024). Techniques and applications for adaptive resource management in reconfigurable computing. SCCTS Transactions on Reconfigurable Computing, 1(1), 6-10. https://doi.org/10.31838/RCC/01.01.02
15. Farhani, M. J., & Jafari, A. A. (2025). Fabrication of micro and nano electro mechanical systems technology for next generation sensors. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(2), 27–35. https://doi.org/10.31838/JIVCT/02.02.04