GRADIVA

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

Edge AI-Driven Lightweight Intrusion Detection for Underwater IoT Wireless Sensor Networks: Enhancing Adaptability, Efficiency, and Real-Time Security

S. Arivumani Samson[1] & Dr. M. Nagarajan[2]

1. Research Scholar, Department of ECE, Bharath Institute of Higher Education and Research, Chennai.
Email: samson@arunai.org
2. Associate Professor, Department of ECE, Bharath Institute of Higher Education and Research, Chennai.
Email: mnagarajan.ece@bharathuniv.ac.in

Abstract

The utilization of Underwater Internet of Things Wireless Sensor Networks (UIoTWSN) is important for the management of resources, monitoring marine environment and conducting environmental evaluations. They dynamic nature of underwater habitats and the limits of Intrusion Detection System are available and provide few obstacles. Because the traditional approach frequently suffers from high computing complexity, raised false positive rates and energy inefficiency, they are not efficiently suited for use in underwater networks that have limited resources. An Edge AI driven Lightweight Intrusion Detection System (Edge-AI IDS) for UIOTWSN is proposed in this study. This method also overcome the issues in the existing methods. The system makes use of method that are based on TinyML such as MobileNetV3 and Gated Recurrent Units for real time detection at edge nodes. Hence, it reduces the amount of processing overhead. Both dynamic transfer learning and meta learning are employed into the system to enhance the adaptability and enables the system to react with evolving threats. To refine decision making, a context aware detection method modifies the sensitivity of the system based in environmental conditions, which reduce the number of false positives. Moreover, techniques that are effective in energy consumption such as quantization and neural network are utilized to conserve power without managing detection accuracy. The decentralized nature of framework uses federated learning and blockchain technology, which ensure the confidentiality of data. It also ensures that network nodes can communicate safely with one another. The result of the experiments shows that the proposed method achieved high accuracy rate and reduced false positive rates in comparison with existing approaches. The proposed method is both scalable and robust for the protection of underwater networks.

Keywords: *Edge AI, UIoTWSNs, Intrusion Detection, TinyML, MobileNetV3, GRU, Federated Learning, Energy Efficiency, Blockchain.*

1. INTRODUCTION

Underwater Internet of Things Wireless Sensor Networks (UIoTWSN) has evolved as a result of rapid enhancement of IoT which has allowed it to expand its reach into places that are submerged in water.

The importance of these networks has grown significantly in different applications such as environmental evaluation, maritime monitoring and underwater exploration. UWIoTWSN provide real time data collection and monitoring as result of their utilization of integrated underwater sensors. This enhances the understanding of ocean ecosystems.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

However, the implementation of UIoTWSN provides different issues specifically with regard to security of the network and energy efficiency. Existing Intrusion Detection system (IDS) have difficult time adapting to the extremely dynamic and resource constrained environment in underwater. These existing systems depends on computationally intensive deep learning methods, which require a large amount of energy and processing power.

Moreover, the existing methods have difficult time to new and emerging threats, which leads to increased false positive rates. It can result in unnecessary disruption to the networks and energy waste. Additionally, this creates additional communication overhead.

An Edge driven lightweight intrusion detection system (Edge AI-IDS) is proposed for addressing the issues in edge artificial intelligence. The proposed method makes use of machine learning method which are both efficient and lightweight. These methods are installed directly on underwater sensor nodes which enable real time detection without the need for centralized data aggregation.

The proposed method also utilizes Mobile Net V3 and Gated recurrent Unit (GRU) in less reduction in both computational complexity and energy usage. It is possible for the method to quickly adapt to new attacks with less training due to utilization of meta learning and dynamic transfer learning. This allows the system to overcome the adaptability limits that are associated with static methods.

To enhance the accuracy detection, a context related detection method has implemented. This method considers aspects such as water and temperature to reduce the number of false positives.

Moreover, the proposed method employs a fully decentralized method using federated learning. This framework allows each sensor node to train its method locally and only communicate encrypted updates, therefore protecting the confidentiality of data. It also reduces cost with transmission.

An environment for integration is provided by the incorporation of blockchain method which ensures the communication between nodes which is constant and secure over time. Energy efficient methods like neural network and quantization is implemented to optimize the resource usage which leads to operational life of underwater networks.

The purpose of this study is to demonstrate that an Edge AI-IDS is a scalable flexible and resource efficient to the specific difficulties with UIoTWSN. The contribution of woks is as follows:

a) One of the most essential contribution is the implementation of lightweight AI methods for real time IDS at edge. It helps to reduce the amount of computational labor needed and enhance the response time.

b) The adaptive learning methods such as meta learning and transfer learning are used to allow rapid adaptation to constant threats.

c) The implementation of detection method is context related and reduces the number of false positives by considering the environmental factors

d) Decentralized Federated Learning method is used with blockchain method for ensuring the confidentiality and privacy of communication.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

The remainder of this paper is structured as follows: Section 2 reviews related work in the domain of underwater intrusion detection systems. Section 3 details the proposed Edge AI-Driven Intrusion Detection methodology. Section 4 presents experimental results and evaluates the performance of the proposed system. Finally, Section 5 concludes the paper and discusses potential directions for future research.

2. RELATED WORKS

Table 1: Existing works on UWIOTWSN using different methods

Reference Number	Technique used	Merits	Demerits
[1]	CNN-GRNN	One of the efficient methods	Less secured method
[2]	Improved Grey Wolf Optimization	Search node in the process has highest accuracy and convergence.	Less localization accuracy is obtained
[3]	Elliptical curve cryptography	The utilization of this method allows for safe exchange of data in UWSN which has different applications in fields of oceanography, military operations and environmental monitoring.	There is no practical implementation
[4]	Support Vector Machine-Dempster-Shafer	It is possible to reduce the probability to incorrect identifying nodes. It also has efficient result in harmful detection	
[5]	Sea Lion Optimization	This algorithm locates the targeted best position to arrange the network in most effective manner considering the highest possible connectivity rate.	Less scalable method
[6]	Random forest	This method can identify malicious nodes and attack types in network as effective manner.	
[7]	convolutional LSTM network with NADAM optimizer	Even this method has environmental variation, this method continues to ensure the reliable Intrusion detection.	One key limitation is its potential difficulty in distinguishing between very similar attack patterns, such as blackhole and TDMA attacks, which suggests a need for further refinement in feature extraction and classification
[8]	Density-Based Spatial Clustering of Applications with Noise	The detection accuracy rate can be effectively improved by this algorithm (ranging from 3% to 15 %). It can also reduce the false positive rate	Less type of attack are only analyzed
[9]	Adaptive random forest	This method obtained highest accuracy of performance using SVM detectors	High computational process
[10]	Generative Adversial network +LSTM	This work employs processes for signal jamming, neighbor based packet monitoring and alarm messaging to develop dependable security system which can obtain different attacks.	Data reliability is less

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

3. PROPOSED METHODOLOGY

The proposed Edge-AI IDS is developed in this study for protecting the UIoTWSN. This method overcomes the issues posed by dynamic underwater environments, evolving threats and resource limits. It makes use of lightweight machine learning methods, energy efficient steps and adaptive learning methods. The implementation of method based onTinyML directly at edge node is essential component of the proposed method.

This method has objective with a smaller number of computational resources. It enables the processing of data in real time without the need on centralized servers. Within Edge AI-IDS, an integration of MobileNetv3 for the extraction of spatial features and Gated Recurrent Unit (GRU) for the detection of temporal pattern is used.

The framework of MobileNetV3 and its efficiency in extracting spatial features from underwater sensor leads to its selection as optimal solution. A representation of convolutional operation in MobileNetV3 is as follows

$$C_{i,j} = \sigma(\sum_{m=1}^{k}\sum_{n=1}^{l} X_{i+m.j+n}.W_{m,n} + b) \quad (1)$$

Where

- $C_{i,j}$ is the output feature map at position (i, j),
- X is the input matrix (sensor data),
- W is the filter (kernel) matrix size
- b is the bias term,
- sigma is the activation function (e.g., ReLU)

Bottle neck layers and depth wise separable convolutions are utilized in the MobileNetV3 framework to reduce the amount of computing required while still preserving accuracy. For identifying temporal dependencies in network traffic data, GRU is utilized.

Because the GRU formulation is less complicated than LSTM, it is better suited for use in resource constrained underwater nodes. The equation of GRU cell is as follows,

$$z_t = \sigma\,(W_z.x_t + U_z.h_{t-1} + b_z) \quad (2)$$

$$r_t = \sigma\,(W_r.x_t + U_r.h_{t-1} + b_r) \quad (3)$$

$$\tilde{h}_t = \tanh(W_h.x_t + r_t \odot (U_r.h_{t-1}) + b_h \quad (4)$$

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad (5)$$

Where:

- x_t is the input at time step t ,
- h_t is the hidden state at time step t ,
- z_t is the update gate, controlling the flow of information,
- r_t is the reset gate, determining how much past information to keep,
- W , U , and b are the weight matrices and biases for the respective gates,
- $\odot$ denotes element-wise multiplication.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

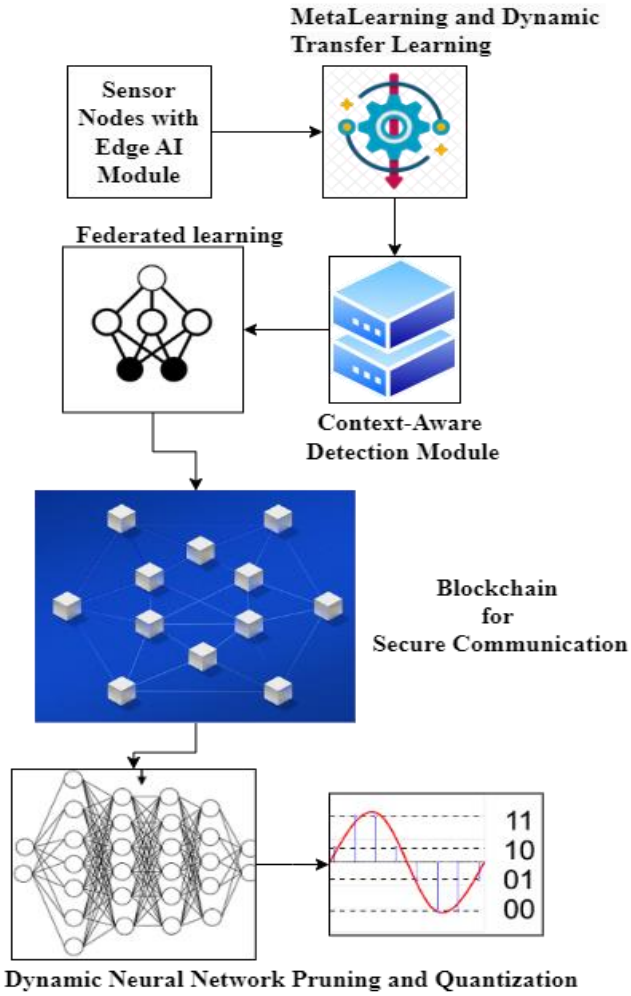

Figure 1: Proposed framework

To improve detection accuracy, an ensemble learning approach is employed. The outputs from MobileNetV3 and GRU are combined using a weighted voting scheme:

$$D_{final} = \arg\max(\sum_{i=1}^{N} w_i . D_i)(6)$$

Where

- $D_{final}$is the final decision (intrusion or normal),
- D_i is the decision from the i-th model,
- w_i is the weight assigned to the i -th model,
- N is the number of models in the ensemble.

Considering the results of different methods, this ensemble method helps to reduce the number of false positives. The system makes use of adaptive learning to manage with dynamic underwater environment and that hazard which are constantly emerging. Through the application of transfer learning, pre trained methods can be adapted to new method with small amount of data. Every node begins with a base method which has been trained worldwide, by M_{global} and uses localized data denoted byD_{local} to fine tune it.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

$$M_{local} = M_{global} + \Delta M (7)$$

Where:

- M_{local} is the fine-tuned model for the specific node,

-ΔMrepresents the local adjustments using D_{local}

This reduces the need for large datasets and enables faster adaptation to new threats.

The integration of meta learning enables each node to generalize rapidly while require few updates at same time. It is also referred as learning to learn. Meta learning acts as following function as its objective

$$\theta^* = \arg\min \sum_{i=1}^{N} \mathcal{L}(M_\theta^i(D_{local}^i), y^i)(8)$$

Where:

- $\theta^*$are the parameters of the model,

- $\mathcal{L}$ is the loss function,

- D_{local}^i is the local dataset for the i -th node,

-y^i is the target output.

- This technique ensures that each model can quickly adapt to new conditions with minimal adjustments, enhancing overall robustness.

A Context-Aware Detection Module refines detection decisions by considering environmental factors: The module uses environmental sensors to gather data on parameters like water temperature, salinity, and pressure.

- An adaptive threshold $T_{adaptive}$is calculated based on these factors:

$$T_{adaptive} = T_{base} + \alpha . f(E)(9)$$

Where:

- T_{base} is the base threshold for detection,

-$f(E)$ is a function of environmental factors E,

- α is a weighting factor determining the influence of the environment on detection sensitivity.

This module reduces false positives by distinguishing between actual intrusions and benign environmental anomalies.

To optimize resource usage, energy-efficient strategies are integrated:

The system uses Dynamic Neural Network Pruning, where unnecessary neurons are pruned based on importance scores, reducing the computational load:

$S_i = \frac{\partial \mathcal{L}}{\partial w_i}(10)$

Where:

- S_i is the importance score for the neuron with weight w_i

- Neurons with scores below a threshold are pruned.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

Quantization reduces the precision of weights from 32-bit floating-point to 8-bit integers, saving memory and computation without a significant accuracy drop.

To ensure privacy and secure communication, a Federated Learning and Blockchain framework is implemented: Each node locally trains its model and shares encrypted updates with a central aggregator:

$$W^{t+1} = W^t + \frac{1}{k}\sum_{k=1}^{k} \Delta w_k (11)$$

Where:

- $W^{t+1}$is the updated global model,
- K is the number of nodes,
- Δw_k is the weight update from the k -th node.

Communication between nodes in blockchain network is ensured to be safe and constant. The validation of each detection decision and update is accomplished through the use of consensus mechanism such as proof of stake (POS) which is recorded in a block. For providing strong solution ensuring UIOTWSN, the Edge AI-IDS is proposed using adaptive learning and energy efficient methods.

Based on the utilization of federated learning and blockchain method, the method not only enhances the precision and adaptability of detection, but it also ensures the confidentiality of data and safe communication in environment which are complex to navigate underwater.

4. EVALUATION METRICS

UNSW-NB15 dataset is used. This dataset was developed by the Australian Centre for cyber security and it contains a different contemporary attack and actual network behaviors. Even it is not designed for underwater networks, Several metrics are utilized to evaluate the performance of the proposed Edge AI IDS.

These metrics are utilized to evaluate the effectiveness of the system in terms of accuracy, efficiency, adaptability and resource utilization. The key metrics for evaluation is as follows, it may be appropriate for adaption due to the increase of attack it can perform.

4.1 Accuracy (Acc)

Accuracy measures the overall effectiveness of the intrusion detection system by calculating the ratio of correctly identified instances (both true positives and true negatives) to the total number of instances:

$$\text{Accuracy} = \frac{\text{Total Instances (TP + TN + FP + FN)}}{\text{True Positives (TP)+True Negatives (TN)}} (12)$$

Where,

TP indicates true positive

FP indicates false positive

TN indicates true negative

FN indicates false negative

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

Table 2: Comparison of Accuracy Values

Methods	Accuracy
convolutional LSTM network with NADAM optimizer [7]	98.24%
Density-Based Spatial Clustering of Applications with Noise [8]	90.7%
Adaptive random forest [9]	89.1%
Generative Adversial network +LSTM [10]	92.4%
Proposed	98.5%

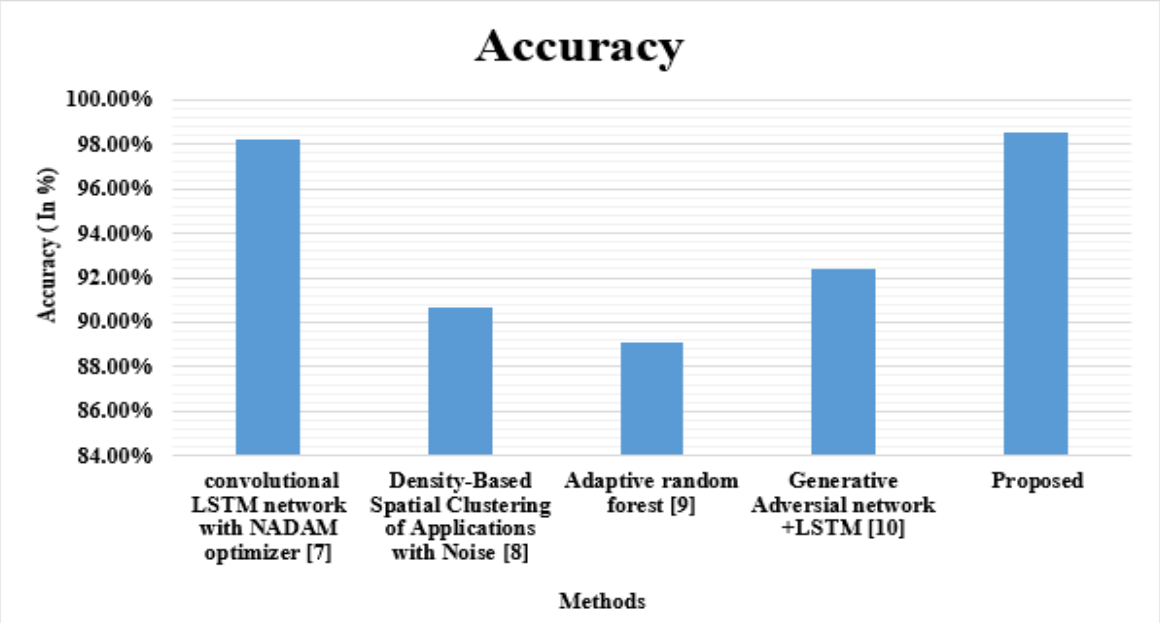

Figure 2: Accuracy analysis

The accuracy values of the proposed Edge AI-IDS and the existing IDS in underwater networks are compared in Figure 2. To determine the capability of system to accurately identify both intrusion and normal network activities, accuracy is an essential parameter is evaluated. The results in the figure shows that the proposed Edge AI-IDS achieves a higher accuracy of 98.5% compared to other methods such as the Adaptive Random Forest at 90.62% and the LSTM based system at 91.2%. It shows that the lightweight methods such as GRU and MobileNetV3 are able to reliably detect attacks inside the complex and dynamic underwater environment.

4.2 Precision (P)

Precision assesses the proportion of correctly predicted intrusion events out of all predicted positive events. It evaluates the system's ability to minimize false positives:

$$\text{Precision} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False positivites}} \quad (13)$$

Table 3: Comparison of Precision Values

Methods	Precision
convolutional LSTM network with NADAM optimizer [7]	89.15%
Density-Based Spatial Clustering of Applications with Noise [8]	92.1%
Adaptive random forest [9]	90.5%
Generative Adversial network +LSTM [10]	94.3%
Proposed method	96.2%

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

A high precision score indicates fewer false alarms, making the system more reliable for real-world applications where false positives could lead to unnecessary actions.

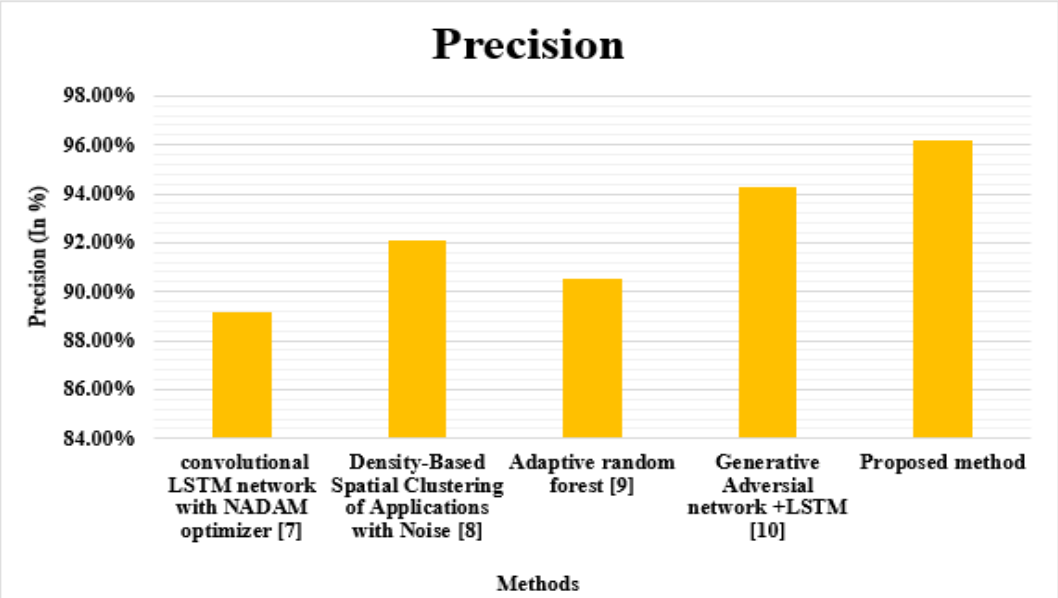

Figure 3: Precision analysis

Figure 3 presents a comparative analysis of precision values obtained by various intrusion detection method including proposed Edge AI-IDS. The suggested Edge AI-IDS has the greatest precision score of 96.2% outperforming other methods such as Adaptive random forest (90.5%) and the CNN-LSTM (92.1%).

With high precision, it is clear that proposed Edge AI-IDS is extremely efficient in reducing the number of false positives. This proposed method is an efficient for real time applications in underwater situations, where the unnecessary alerts could potentially create disturbances.

4.3 Recall (R)

Recall, also known as Sensitivity or True Positive Rate (TPR), measures the ability of the system to correctly identify intrusions. It is the ratio of true positives to the total actual intrusions:

$$\text{Recall} = \frac{\text{True Positives (TP)}}{\text{TruePositives (TP)+False Negativites}} \quad (14)$$

Table 4: Comparison of Recall Values

Methods	Recall
convolutional LSTM network with NADAM optimizer [7]	89.32%
Density-Based Spatial Clustering of Applications with Noise [8]	89.3%
Adaptive random forest [9]	87.6%
Generative Adversial network +LSTM [10]	91.2%
Proposed method	94.8%

A higher recall value indicates that the system is effective at detecting most of the intrusion attempts.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

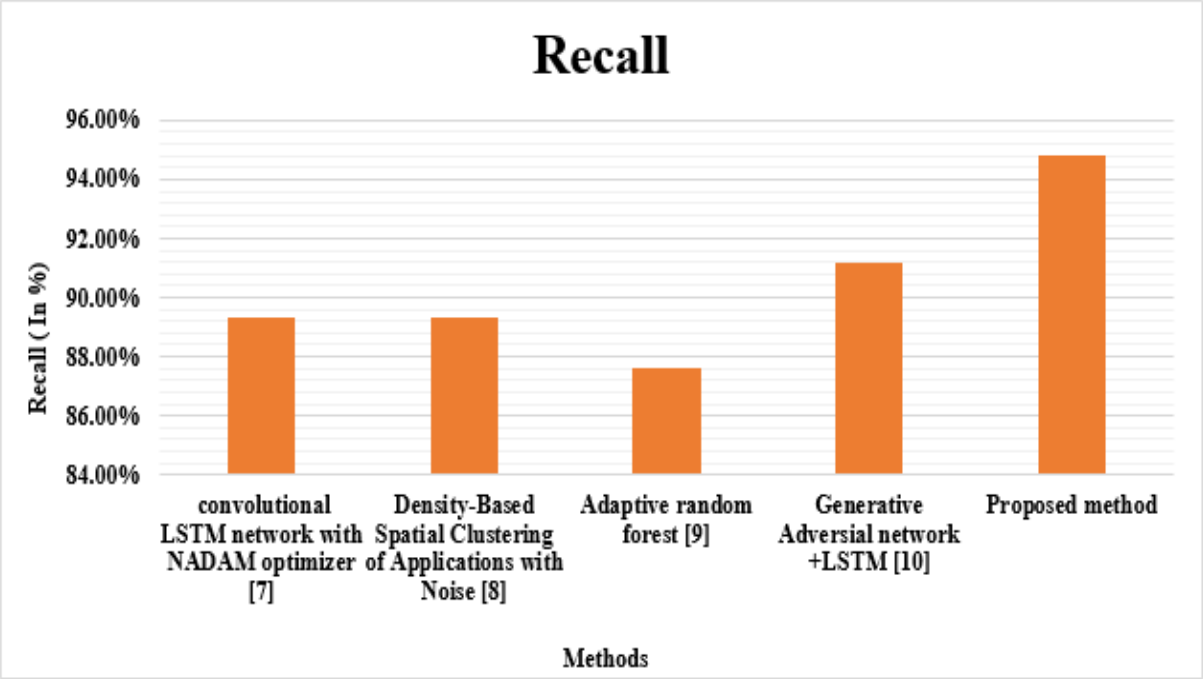

Figure 4: Recall analysis

The recall values of the proposed Edge AI-IDS are compared with existing IDS in figure 4. The proposed Edge AI-IDS obtained recall score of 94.8% while the Adaptive random forest obtains 87.6% and GAN-LSTM achieves 91.2%.

Based on high recall, it can be demonstrated that the proposed Edge AI-IDS is capable of effectively detecting wider variety of intrusion types. It hence reduces the risk of missed threats. The application of adaptive leraning methods enables the method to dynamically react to changing attack patterns. It ultimately result in enhanced recall performance.

4.4 F1-Score

F1-Score is defined as the average value between precision and recall.

$$\mathrm{F1-Score} = 2 \times \frac{\mathrm{Precision+Recall}}{\mathrm{Precision \times Recall}} \quad (15)$$

Table 5: Comparison of F1-score values

Methods	F1-Score
convolutional LSTM network with NADAM optimizer [7]	99.16%
Density-Based Spatial Clustering of Applications with Noise [8]	90.6%
Adaptive random forest [9]	88.9%
Generative Adversial network +LSTM [10]	92.7%
Proposed method	99.3%

A high F1-Score ensures that the system not only detects intrusions accurately but also minimizes false alarms.

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

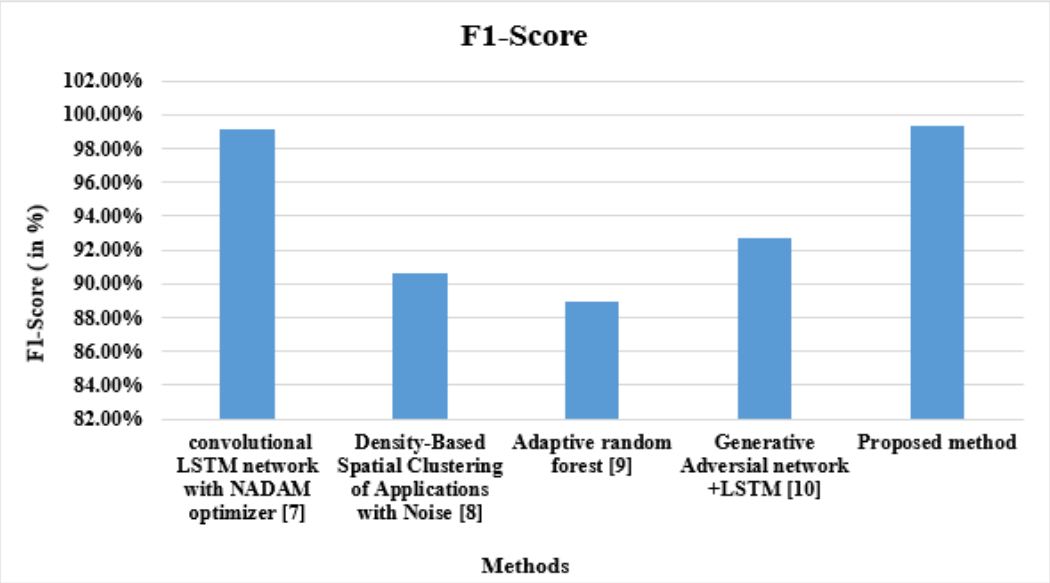

Figure 5: F1-Score analysis

Figure 5 shows the f1-score analysis of different IDS with proposed Edge AI-IDS. The figure demonstrates that the proposed Edge AI-IDS has the highest F1-Score of 99.3% exceeding other methods such as Adaptive random forest (88.9%) and Convolutional LSTM network (86.8%). It demonstrated that the Edge AI-IDS maintains high accuracy and manages the balance between recall and precision values. It is a reliable method for identifying difficult patterns in underwater networks environments in which it is necessary to reduce the number of false positives and false negatives.

5. CONCLUSION

The proposed Edge AI driven Lightweight IDS for UIoTWSN to address the significant issues with protection of underwater environments. Intrusion Detection System (IDS) are more traditional frequently issues with significant false positive rate, energy inefficiency and high computing complexity. The proposed method is effective at real time detection utilizing lightweight artificial intelligence methods like Mobile Net V3 and GRU. This considerably reduces the amount of computational work which is needed. Dynamic transfer learning and meta learning are two examples of adaptive learning employed into system. These methods allow the system to rapidly adjust to new and evolving threats. The context related detection method improves decision making by considering environmental factors which in reduces the number of false positives. Moreover, energy efficient methods such as neural network and quantization are used to optimize resource utilization. It results in enhancement of network life. Through the utilization of federated learning and blockchain method, the decentralized architecture ensures the confidentiality of data and privacy of communication between nodes. The findings of the result demonstrates that the proposed Edge AI-IDS performs better than standard approaches in terms of energy efficiency, precision, accuracy and recall. This method provides scalable and robustness for the protection of underwater networks. In the future, the work will be focused on improving the flexibility of system to different underwater circumstances and enhancing its scalability so that it can accommodate larger networks

Volume 64 | Issue 02 | February 2025
DOI: 10.5281/zenodo.14856202

References

1) Manoharan, J. S. et al. (2023). A novel hybrid machine learning approach for traffic sign detection using CNN-GRNN. Journal of Intelligent and Fuzzy Systems. 44:1283-1303. https://doi.org/10.3233/JIFS-221720.

2) Jeyaseelan, W.S., Jayasankar, T., Kumar, K.V. and Ponni, R., 2024. Improved Grey Wolf Optimization Based Node Localization Approach in Underwater Wireless Sensor Networks. *Measurement Science Review*, *24*(3), pp.95-99.

3) Shah, S., Munir, A., Waheed, A., Alabrah, A., Mukred, M., Amin, F. and Salam, A., 2023. Enhancing security and efficiency in underwater wireless sensor networks: a lightweight key management framework. *Symmetry*, *15*(8), p.1484.

4) Su, Y., Ma, S., Zhang, H., Jin, Z. and Fu, X., 2021. A redeemable SVM-DS fusion-based trust management mechanism for underwater acoustic sensor networks. *IEEE sensors journal*, *21*(22), pp.26161-26174.

5) Kumar Gola, K., Chaurasia, N., Gupta, B. and Singh Niranjan, D., 2021. Sea lion optimization algorithm based node deployment strategy in underwater acoustic sensor network. *International Journal of Communication Systems*, *34*(5), p.e4723.

6) Jiang, B., Zhou, R., Luo, F., Cui, X., Liu, Y. and Song, H., 2024. Hybrid Trust Model for Identifying Malicious Attacks in Underwater Acoustic Sensor Network. *IEEE Sensors Journal*.

7) Arivumani Samson.S. and Nagarajan, M., 2024. Adaptive convolutional-LSTM neural network with NADAM optimization for intrusion detection in underwater IoT wireless sensor networks. *Engineering Research Express*, *6*(3), p.035243.

8) Zhang, R., Zhang, J., Wang, Q. and Zhang, H., 2023. DOIDS: an intrusion detection scheme based on DBSCAN for opportunistic routing in underwater wireless sensor networks. *Sensors*, *23*(4), p.2096.

9) Das, S., Pasikhani, A.M., Gope, P., Clark, J.A., Patel, C. and Sikdar, B., 2023. AIDPS: Adaptive Intrusion Detection and Prevention System for Underwater Acoustic Sensor Networks. *IEEE/ACM Transactions on Networking*.

10) Rajasoundaran, S., Kumar, S.S., Selvi, M., Thangaramya, K. and Arputharaj, K., 2024. Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. *Wireless Networks*, *30*(1), pp.209-231.