ALO-IDChain: Ant Lion Optimized DL Model for Intrusion Detection with Blockchain Logging in IoMT

Subroto Kumar Ghosh, Mohtasin Golam, Sium Bin Noor, Jae-Min Lee, and Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(subroto, gmoh248, siumbinmoor, ljmpaul, and dskim)@kumoh.ac.kr

***Abstract*—The growing use of Internet of Medical Things (IoMT) devices has brought valuable benefits to healthcare but also introduced serious security risks. These devices handle sensitive patient data and often operate under limited computational resources, making them attractive targets for cyberattacks. In this paper, a lightweight yet effective intrusion detection system ALO-IDChain is introduced that combines deep learning, feature optimization, and blockchain technology. The Ant Lion Optimizer (ALO) reduces the feature space from 52 to 25, cutting down complexity while retaining important information. These selected features are used to train a Time Series Transformer model designed to detect intrusions in IoMT traffic. When compared with a baseline model using all features, the ALO-enhanced version achieved slightly higher accuracy (99.89%), precision (0.9974), and F1 score (0.9987), while also reducing computational cost. The training time was reduced from 1260.22s to 1182.08s, and the inference time per sample dropped from 0.3010ms to 0.1609ms, making the model well suited for real-time applications. To make intrusion detection more transparent and verifiable, the system logs attack's information onto a permissioned blockchain called Pure Chain. This ensures that once an intrusion is detected, the event is permanently and securely recorded. Together, these components form a practical and trustworthy framework for securing IoMT environments. The system not only detects threats accurately but also builds a tamper-proof trail of evidence for future auditing.**

***Index Terms*—Ant Lion Optimizer, Intrusion Detection, IoMT, Pure Chain, Time Series Transformer.**

I. Introduction

The Internet of Medical Things (IoMT) is an evolving technology that integrates a network of interconnected medical devices, sensors, and systems to continuously monitor and collect real-time health data for medical purposes [1]. This interconnected ecosystem of devices enables healthcare providers to access continuous, real-time data streams, enhancing decision making capabilities and promoting a more proactive approach to patient care. This system significantly enhances healthcare facilities by enabling timely and accurate disease detection, promoting early intervention, and reducing healthcare costs [2]. By automating many processes, IoMT reduces the administrative burden on healthcare facilities, which can result in significant cost savings across healthcare systems. IoMT devices, such as wearable sensors, provide a seamless means of tracking vital health parameters, enabling healthcare professionals to monitor patients remotely and personalize treatment plans [3], [4], [5]. This not only reduces the burden on healthcare facilities but also improves patient outcomes by providing more accessible and efficient care, especially for patients with chronic conditions [6], [7].

However, the rapid advancement of IoMT technologies brings substantial benefits but also introduces significant security risks [8]. Cyberattacks targeting IoMT infrastructures can lead to unauthorized access to sensitive medical data, manipulation of device functions, or denial-of-service (DoS) attacks that disrupt critical healthcare operations [9]. These vulnerabilities extend beyond technical challenges, posing serious threats to patient safety and undermining trust in digital healthcare systems [10]. Developing effective security mechanisms for IoMT is particularly challenging due to the resource constraints of many medical devices and the diverse nature of the data they generate. Traditional intrusion detection systems (IDS), which rely on signature based methods or shallow machine learning models, often struggle with scalability, adaptability, and the ability to generalize to new attack patterns [11]. Furthermore, these systems frequently demand large sets of features, making them computationally expensive and unsuitable for real-time deployment in resource-constrained environments. As the adoption of IoMT continues to grow, there is an urgent need for intelligent, efficient, and verifiable solutions that can effectively protect these systems.

To address these challenges, this paper proposes **ALO-IDChain**, a novel framework for intrusion detection in IoMT networks that integrates three key technologies: feature selection using the *Ant Lion Optimizer (ALO)* [12], a deep learning model based on the *Time Series Transformer* architecture, and tamper-proof attack logging using a permissioned blockchain. The goal is to create a system that is not only accurate and lightweight but also capable of providing trustworthy and transparent intrusion records. In this framework, ALO-based feature selection reduces the dimensionality of the dataset while retaining high-impact features. ALO selects an optimal subset of features for training, substantially reducing computational overhead while maintaining high classification performance. The second component is a *Time Series Transformer*, a deep learning model designed to capture temporal patterns in sequential data. Unlike recurrent neural networks (RNNs) or convolutional neural networks (CNNs), transformers use self-attention mechanisms that better model long range dependencies in time series data. It makes them particularly suitable for analyzing IoMT traffic flows, which often contain latent temporal features indicative of intrusions. To enhance

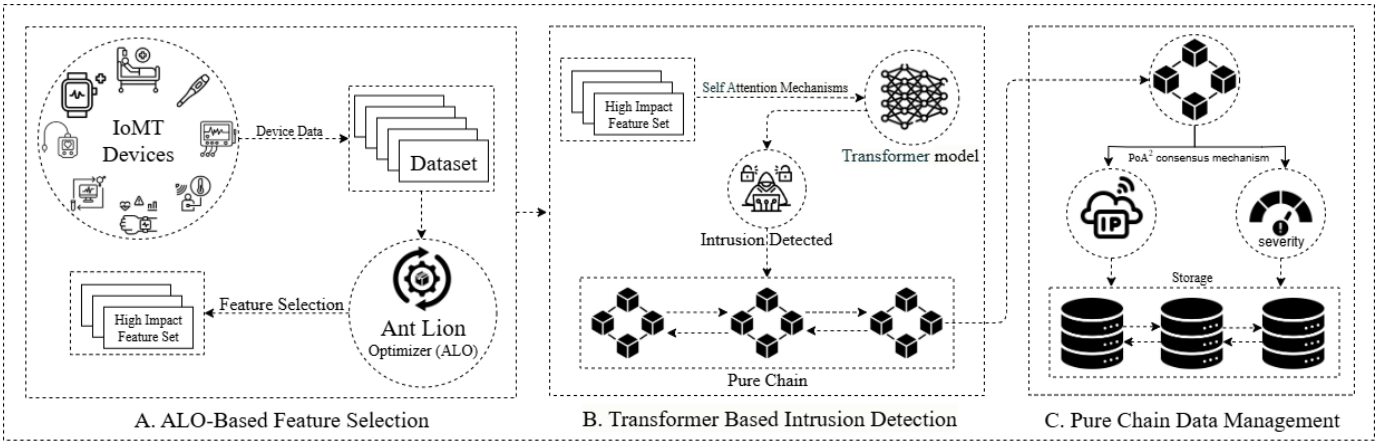

Fig. 1: System Architecture of the Proposed ALO-IDChain

trust and accountability, the third component of this framework introduces a blockchain-based logging system. Once an intrusion is detected, the system automatically records the attack's source IP and severity on *Pure Chain*, a permissioned blockchain using PoA^2 consensus mechanism [13], [14]. This ensures that each detection event is immutably stored and can be audited or traced later if needed. By integrating blockchain into the detection loop, the system bridges the gap between technical security and organizational accountability [15], [16].

To summarize, this work makes the following contributions:

- Applied the Ant Lion Optimizer for lightweight feature selection, improving performance while reducing the cost of deep learning inference.
- Developed a transformer-based model tailored for time series intrusion detection in IoMT networks.
- Integrated a blockchain-based logging mechanism to ensure secure, auditable, and decentralized storage of intrusion alerts.

Together, these components make ALO-IDChain a complete and practical solution for safeguarding IoMT environments against evolving cyber threats.

II. Methodology

Figure 1 illustrates the complete system design and implementation workflow of the proposed ALO-IDChain framework for intrusion detection and blockchain based logging in IoMT systems. The entire methodology was executed in a GPU-enabled virtual environment using Jupyter Notebook, VS Code and Remix IDE.

A. Dataset Description and Preprocessing

The IoT Healthcare Security Dataset [17] was utilized which consists three files: *Attack.csv*, *patientMonitoring.csv*, and *environmentMonitoring.csv*. These files were concatenated and shuffled, resulting in a final dataset with 188,684 samples and 52 features. The target variable `label` denotes normal traffic (0) and attack traffic (1). Categorical features in the dataset were transformed using frequency encoding to avoid dimensionality explosion caused by one-hot encoding. The encoded dataset was then normalized using the `StandardScaler` to ensure uniform feature scaling. To convert the data into a suitable format for time series processing, a sliding window approach was applied. Specifically, a window size of 10 and step size of 1 were used to segment the data into sequences, resulting in three-dimensional tensors `X_seq` and labels `y_seq`.

B. Model Architecture: Time Series Transformer

A deep learning model based on the Time Series Transformer architecture was adopted. It is designed to capture long-range temporal dependencies in IoMT traffic data. The architecture consists of the following components:

- **Input Projection Layer:** Given input sequence $\mathbf{X} \in \mathbb{R}^{B\times T\times F}$, each vector $\mathbf{x}_t \in \mathbb{R}^F$ is projected to a d-dimensional space:

$$\mathbf{h}_t = \mathbf{W}_p\mathbf{x}_t + \mathbf{b}_p \tag{1}$$

- **Positional Encoding:** To inject temporal information, sinusoidal encodings are added:

$$\mathrm{PE}_{(pos,2i)} = \sin\left(\frac{pos}{10000^{2i/d}}\right) \tag{2}$$

$$\mathrm{PE}_{(pos,2i+1)} = \cos\left(\frac{pos}{10000^{2i/d}}\right) \tag{3}$$

- **Transformer Encoder:** Each encoder layer applies Multi-Head Self-Attention (MHSA) and a feedforward network:

$$\mathrm{MHSA}(\mathbf{Q},\mathbf{K},\mathbf{V}) = \mathrm{Concat}(\mathrm{head}_1,\ldots,\mathrm{head}_h)\mathbf{W}^O \tag{4}$$

where each head is:

$$\mathrm{head}_i = \mathrm{Attention}(\mathbf{Q}\mathbf{W}_i^Q, \mathbf{K}\mathbf{W}_i^K, \mathbf{V}\mathbf{W}_i^V) \tag{5}$$

- **Global Pooling:** Average pooling aggregates all temporal embeddings:

$$\mathbf{z} = \frac{1}{T}\sum_{t=1}^{T}\mathbf{h}_t \tag{6}$$

C. ALO-Based Feature Selection

To reduce computational overhead and enhance real-time inference efficiency in the intrusion detection framework, the Ant Lion Optimizer (ALO), a nature-inspired metaheuristic algorithm, was employed. This algorithm is known for its balance between exploration and exploitation. ALO simulates the hunting mechanism of antlions in nature, where the optimization process is driven by the stochastic interaction between antlions (representing candidate solutions) and ants (representing the search process).

The primary goal of ALO in this context was to identify the most informative subset of features from the original 52-dimensional dataset. Each candidate solution is encoded as a binary vector:

$$\mathbf{X} = [x_1, x_2, \ldots, x_n], \quad x_i \in \{0, 1\}, \quad n = 52 \tag{7}$$

where $x_i = 1$ denotes the inclusion of the i-th feature and $x_i = 0$ its exclusion.

To evaluate the quality of each feature subset, a fitness function was defined using the F1-score of a logistic regression classifier:

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{8}$$

This metric promotes a balance between precision and recall, which is particularly important in imbalanced intrusion detection datasets.

The ALO algorithm operates through iterative random walks influenced by elite and selected antlions. The position of each ant in the feature space is updated as:

$$\mathbf{X}_i^{(t+1)} = \text{Binarize}\left(\frac{\mathbf{RW}_{elite} + \mathbf{RW}_{selected}}{2}\right) \tag{9}$$

where $\mathbf{RW}$ represents the normalized random walk around antlions, and the binarization operator converts the continuous position to binary space using a threshold function. The commonly used sigmoid transfer function for binarization is:

$$\text{Binarize}(z) = \begin{cases} 1, & \text{if } \sigma(z) > r \\ 0, & \text{otherwise} \end{cases} \quad \text{where } \sigma(z) = \frac{1}{1+e^{-z}}, \quad r \sim (0, 1) \tag{10}$$

ALO was configured with a population size of 10 and executed for 10 iterations. The bounds of the problem were initialized using `BinaryVar()` for each of the 52 features, and the objective was set to maximize the average F1-score over 3-fold cross-validation.

The optimal feature subset identified by ALO contained 25 features, significantly reducing the input dimensionality while maintaining high classification performance.

The algorithm proceeds as follows:

Algorithm 1: Ant Lion Optimizer (ALO) for Feature Selection

Input: Number of ants N, maximum iterations T, fitness function `Fit`$(\cdot)$
Output: Best feature subset found

Initialize population of ants and antlions randomly ;
for *each ant and antlion* **do**
  Evaluate fitness using `Fit`$(\cdot)$;
Set elite antlion as the best antlion found ;
for $t \leftarrow 1$ ***to*** T **do**
  for *each ant* i **do**
    Select antlion j using roulette wheel selection based on fitness;
    Perform random walk around selected antlion j and elite antlion;
    Update ant i position accordingly;
    if (binary feature selection) **then** apply thresholding or binarization;
  for *each ant* **do**
    Evaluate fitness using `Fit`$(\cdot)$;
  for *each ant* i **do**
    if *fitness(ant i)* $>$ *fitness(antlion i)* **then**
      Replace antlion i with ant i;
  Update elite antlion if a better solution is found;
return *elite antlion as best feature subset*

Using this approach, ALO selected 25 features that were used to regenerate the time-series tensors for training the Time Series Transformer model. The selected subset retained critical features including temporal, network-level, and MQTT-specific attributes that contributed to the predictive power of the model.

D. Training and Evaluation Setup

The complete pipeline was executed twice: once using all 52 features (baseline model) and once using the subset of features selected by the ALO. For both settings, the dataset was stratified and split into 80% for training and 20% for testing. Training was performed over 10 epochs with a batch size of 64, using the Adam optimizer with a learning rate of 0.001. The model was implemented in PyTorch, and binary classification was conducted using the `BCEWithLogitsLoss` loss function.

Performance was assessed using Accuracy, Precision, Recall, F1-score, Confusion Matrix, ROC Curve, training time and inference time per sample. Additionally, the blockchain component was assessed by measuring gas consumption, confirmation latency, and throughput (TPS) during logging bursts.

E. Blockchain Integration for Intrusion Logging

To ensure tamper-proof logging of detected intrusions, a Solidity based smart contract was deployed on the Pure Chain. The contract structure includes:

- `logIntrusion()`: Logs source IP and severity of detected attack.

- `getEvent()`: Retrieves event details by index.
- `getTotalEvents()`: Returns total number of logged events.

Integration was implemented via Web3.py. Upon detection of an attack ($\hat{y} = 1$), relevant fields such as source IP and severity score were extracted and logged on-chain.

III. Performance Evaluation

In this section, the system performance is analyzed using various metrics. A detailed analysis of the model's performance is provided by comparing the results with and without the use of the Ant Lion Optimizer (ALO).

A. Model Performance Without Using ALO

The baseline model is trained using all 52 features from the dataset. The following results were obtained:

- **Test Accuracy**: 99.71%
- **Precision**: 0.9932
- **Recall**: 1.0000
- **F1-Score**: 0.9966

The confusion matrix for the baseline model is shown in Figure 2. It demonstrates that the model correctly classified nearly all instances of both normal and attack traffic. However, it produced 109 false positives and no false negatives, effectively detecting all attacks but generating more false alerts.

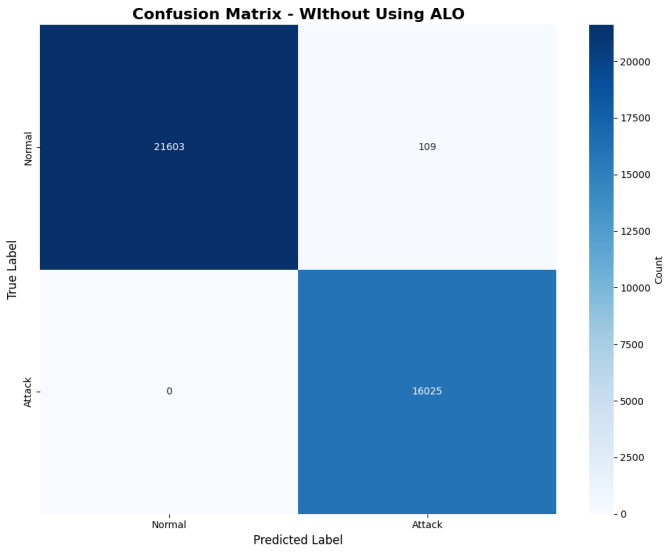

Fig. 2: Confusion Matrix - Without Using ALO

The ROC curve for the baseline model is presented in Figure 3, showing an AUC score of 0.9999. This high value confirms the model's excellent classification performance and ability to distinguish between normal and attack traffic.

B. Model Performance Using ALO

Using ALO for feature selection, we reduce the number of features from 52 to 25. The results obtained with ALO are as follows:

- **Test Accuracy**: 99.89%

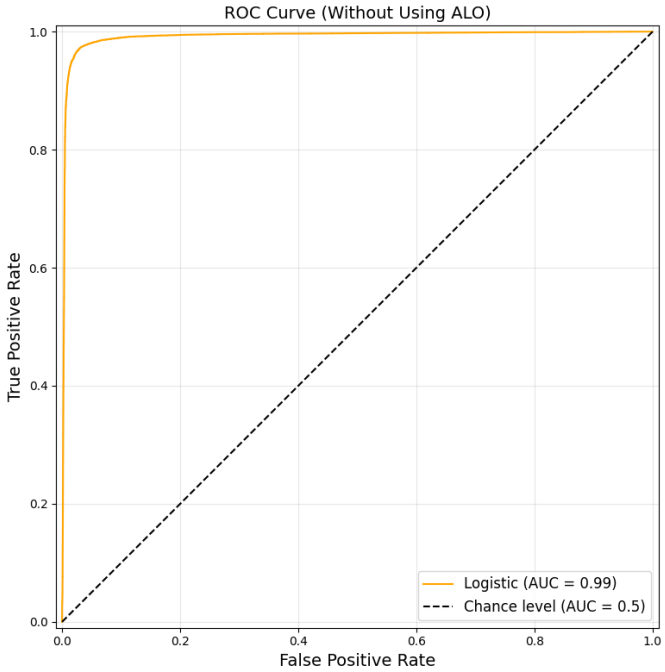

Fig. 3: ROC Curve - Without Using ALO

- **Precision**: 0.9974
- **Recall**: 0.9999
- **F1-Score**: 0.9987

The confusion matrix for the ALO-enhanced model is shown in Figure 4. Compared to the baseline model, this version shows only 41 false positives while maintaining zero false negatives. This indicates improved classification of normal traffic and better overall balance in detection.

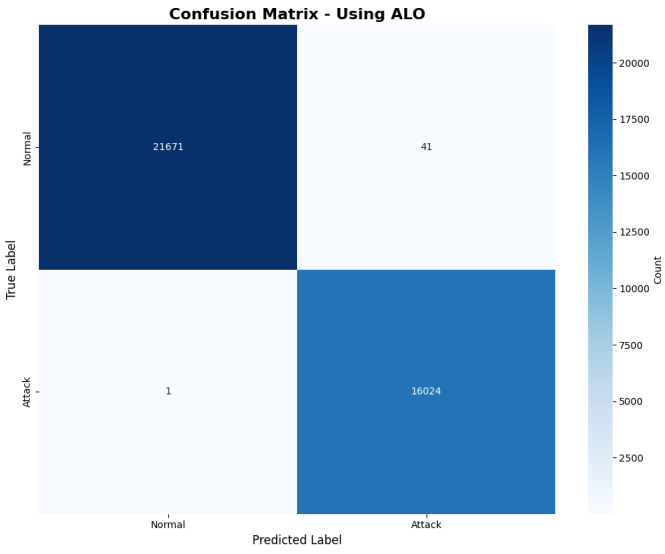

Fig. 4: Confusion Matrix - Using ALO

The ROC curve for the model with ALO is depicted in Figure 5. The AUC value is 0.9990, slightly lower than the

baseline, yet still outstanding. This confirms that ALO-based feature selection retains excellent model discrimination while reducing feature count.

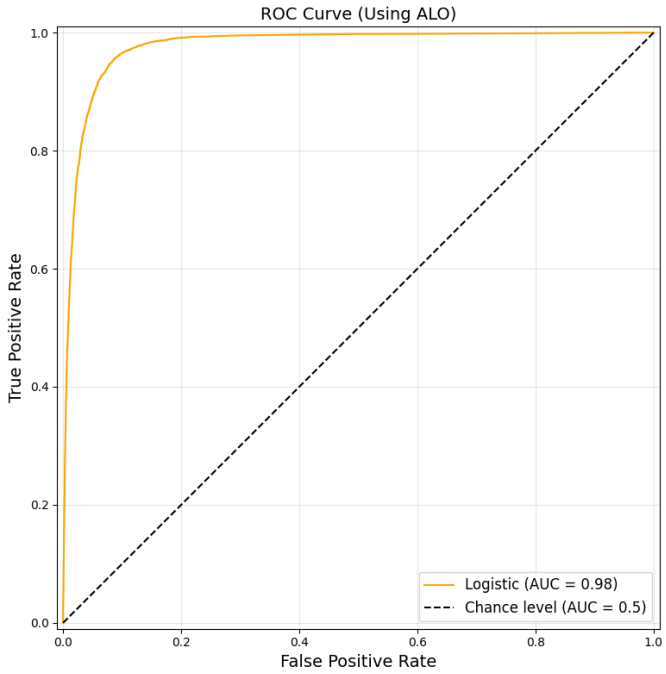

Fig. 5: ROC Curve - Using ALO

C. Comparison of Results

Table I summarizes the performance metrics for both configurations. The ALO-based model exhibits superior efficiency in terms of inference and training times, with slightly improved accuracy and F1-score.

TABLE I: Comparison of Evaluated Models with and without ALO

Metric	Without ALO	With ALO
Accuracy	99.71%	99.89%
Precision	0.9932	0.9974
Recall	1.0000	0.9999
F1-Score	0.9966	0.9987
AUC Score	0.9999	0.9990
Training Time (s)	1260.22	1182.08
Inference Time (ms)	0.3010	0.1609
False Positives	109	41
False Negatives	0	0

D. Blockchain Integration Performance

To enhance transparency and accountability, the ALO-IDChain system logs detected attacks to Pure Chain, ensuring that each intrusion is immutably recorded. Upon detection of an attack, the corresponding **Source IP** and **Severity** are securely transmitted to the blockchain.

This system ensures that detected intrusions are immutably stored on Pure Chain via the `logIntrusion()` function, with each entry traceable through a unique transaction hash.

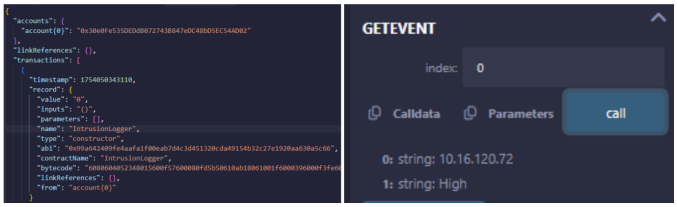

Fig. 6: Transaction Record & Attack Data

Events can be queried using `getEvent()` or enumerated via `getTotalEvents()`, enabling transparent audit trails.

The blockchain layer guarantees tamper-proof and verifiable logging, even if the detection system is compromised. This is especially crucial in healthcare IoMT environments, where data integrity and compliance are paramount.

E. Performance Evaluation on Pure Chain

To assess the efficiency of the blockchain integration, the performance of the `logIntrusion()` function was empirically evaluated using Pure Chain. The summary of performance metrics is presented in Table II.

TABLE II: Performance Metrics of `logIntrusion()` on Pure Chain

Metric	Value
Gas Consumption per Transaction	75,866 gas units
Avg. Confirmation Time (Latency)	1.63 seconds
Confirmation Time Range	1.16 s – 2.40 s
Peak Throughput	10.84 transactions/sec
Burst Test Duration	0.92 seconds (10 transactions)

These results demonstrate that the smart contract operates with consistent and moderate gas usage, confirming its computational efficiency. The average confirmation time of 1.63 seconds ensures near real-time performance, and the achieved transaction throughput of 10.84 tx/sec reflects strong scalability for typical IoMT use cases.

F. Comparison with Recent Works

Table III presents a comparative analysis between ALO-IDChain and recent intrusion detection frameworks. Unlike prior works relying on complex hybrid models (e.g., CNN-LSTM-DQN [18], CNN-LSTM [7]) or GRU-based architectures [19], ALO-IDChain leverages a lightweight Time Series Transformer optimized via the Ant Lion Optimizer (ALO).

ALO-IDChain achieves a higher accuracy, precision, recall, and F1-score, while also reducing feature dimensionality. Furthermore, the integration of Pure Chain for intrusion logging provides verifiable audit trails, which most related works do not address. These results validate ALO-IDChain as a secure, accurate, and efficient solution for real-time intrusion detection in IoMT.

G. Discussion

The ALO-enhanced model demonstrates improved accuracy and reduced false positives compared to the baseline model, making it particularly suited for computationally demanding

TABLE III: Comparison with Recent Works in Intrusion Detection

Author & Year	Feature Selection	Model Type	Blockchain	Accuracy	Precision	Recall	F1-Score
Shaikh et al. (2025) [18]	MIFS	CNN + LSTM + PPO + DQN	Not Used	99.58%	0.9941	0.9994	0.9967
Alamro et al. (2023) [7]	ALO	CNN + LSTM + FPA	Mentioned	99.55%	0.9896	0.9951	0.9923
Yu et al. (2025) [19]	EHO	GRU-based IDS	Not Used	98.50%	0.9750	0.9810	0.9780
ALO-IDChain (Ours)	ALO	Time Series Transformer	Pure Chain	99.89%	0.9974	0.9999	0.9987

IoMT environments. By selecting a smaller subset of features, ALO reduces training time, inference latency, and operational costs. Additionally, the integration of blockchain technology ensures that intrusion detection logs are secure, immutable, and auditable, enhancing data integrity and accountability in healthcare IoMT systems. Performance analysis of the deployed smart contract on Pure Chain revealed moderate gas consumption, low latency, and high throughput, validating its suitability for real-time logging in IoMT.

IV. Conclusion

This paper presented ALO-IDChain, a novel framework for intrusion detection in IoMT environments, integrating Ant Lion Optimizer (ALO) for efficient feature selection, a Time Series Transformer (TST) for temporal analysis, and blockchain-based logging for secure intrusion records. The results demonstrate that ALO improves the model's performance by reducing both training and inference times, making the system more efficient and suitable for real-time deployments. The TST effectively captures long range dependencies in IoMT data, while the Pure Chain ensures tamper-proof and auditable logs of detected intrusions. ALO-IDChain thus provides a lightweight, secure, and scalable solution for real-time intrusion detection in IoMT, ensuring high accuracy and robust data security in healthcare systems. Future work will aim to explore the integration of federated learning to further enhance the scalability and privacy of ALO-IDChain.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] A. Talaminos-Barroso, J. Reina-Tosina, and L. M. Roa, "Adaptation and application of the ieee 2413-2019 standard security mechanisms to iomt systems," *Measurement: Sensors*, vol. 22, p. 100375, 2022.

[2] M. Adil, M. K. Khan, M. M. Jadoon, M. Attique, H. Song, and A. Farouk, "An ai-enabled hybrid lightweight authentication scheme for intelligent iomt based cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2719–2730, 2022.

[3] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured iomt framework based on swarm-neural network," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1969–1976, 2021.

[4] S. Y. Siddiqui, A. Haider, T. M. Ghazal, M. A. Khan, I. Naseer, S. Abbas, M. Rahman, J. A. Khan, M. Ahmad, M. K. Hasan *et al.*, "Iomt cloud-based intelligent prediction of breast cancer stages empowered with deep learning," *Ieee Access*, vol. 9, pp. 146 478–146 491, 2021.

[5] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. ur Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in iomt," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10 125–10 132, 2023.

[6] M. Kumar, S. Verma, A. Kumar, M. F. Ijaz, D. B. Rawat *et al.*, "Anaf-iomt: a novel architectural framework for iomt-enabled smart healthcare system by enhancing security based on recc-vc," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8936–8943, 2022.

[7] H. Alamro, R. Marzouk, N. Alruwais, N. Negm, S. S. Aljameel, M. Khalid, M. A. Hamza, and M. I. Alsaid, "Modeling of blockchain assisted intrusion detection on iot healthcare system using ant lion optimizer with hybrid deep learning," *IEEE Access*, vol. 11, pp. 82 199–82 207, 2023.

[8] A. A. Jolfaei, S. F. Aghili, and D. Singelee, "A survey on blockchain-based iomt systems: Towards scalability," *Ieee Access*, vol. 9, pp. 148 948–148 975, 2021.

[9] A. Aljuhani, A. Alamri, P. Kumar, and A. Jolfaei, "An intelligent and explainable saas-based intrusion detection system for resource-constrained iomt," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25 454–25 463, 2024.

[10] J. Areia, I. A. Bispo, L. Santos, and R. L. d. C. Costa, "Iomt-trafficdata: Dataset and tools for benchmarking intrusion detection in internet of medical things," *IEEE Access*, vol. 12, pp. 115 370–115 385, 2024.

[11] U. Zukaib, X. Cui, C. Zheng, M. Hassan, and Z. Shen, "Meta-ids: Meta-learning-based smart intrusion detection system for internet of medical things (iomt) network," *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 23 080–23 095, 2024.

[12] B. B. Gupta, A. Gaurav, R. W. Attar, V. Arya, S. Bansal, A. Alhomoud, and K. T. Chui, "A hybrid ant lion optimization algorithm based lightweight deep learning framework for cyber attack detection in iot environment," *Computers and Electrical Engineering*, vol. 122, p. 109944, 2025.

[13] D.-S. Kim and R. Syamsul, "Integrating Machine Learning with Proof-of-Authority-and-Association for Dynamic Signer Selection in Blockchain Networks," *ICT Express*, 2024.

[14] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.

[15] S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, M. A. Dini, I. U. Uchechi, D.-S. Kim, and J. M. Lee, "Medical iot record security and blockchain: Systematic review of milieu, milestones, and momentum," *Big Data and Cognitive Computing*, vol. 8, no. 9, p. 121, 2024.

[16] M. F. Rahaman, M. Golam, M. R. Subhan, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Meta-governance: Blockchain-driven metaverse platform for mitigating misbehavior using smart contract and ai," *IEEE Transactions on Network and Service Management*, 2024.

[17] M. Benmalek, A. Seddiki, and K.-D. Haouam, "Snn-iomt: A novel ai-driven model for intrusion detection in internet of medical things," *CMES-Computer Modeling in Engineering and Sciences*, vol. 143, no. 1, pp. 1157–1184, 2025.

[18] J. A. Shaikh, C. Wang, M. W. U. Sima, M. Arshad, M. Owais, D. S. Hassan, R. Alkanhel, and M. S. A. Muthanna, "A deep reinforcement learning-based robust intrusion detection system for securing iomt healthcare networks," *Frontiers in Medicine*, vol. 12, p. 1524286, 2025.

[19] H. Yu, W. Zhang, C. Kang, and Y. Xue, "A feature selection algorithm for intrusion detection system based on the enhanced heuristic optimizer," *Expert Systems with Applications*, vol. 265, p. 125860, 2025.