Bit-by-Bit: A Quantization-Aware Training Framework with XAI for Robust Metaverse Cybersecurity

Ebuka Chinaechetam Nkoro*, Cosmas Ifeanyi Nwakanma†, Jae-Min Lee* and Dong-Seong Kim*,
*IT Convergence Engineering, †ICT Convergence Research Center, Kumoh National Institute of Technology, Korea

***Abstract*—In this work, a novel framework for detecting malicious networks in the IoT-enabled Metaverse networks to ensure that malicious network traffic is identified and integrated to suit optimal Metaverse cybersecurity is presented. First, the study raises a core security issue related to the cyberthreats in Metaverse networks and its privacy breaching risks. Second, to address the shortcomings of efficient and effective network intrusion detection (NIDS) of dark web traffic, this study employs a quantization-aware trained (QAT) 1D CNN followed by fully connected networks (ID CNNs-GRU-FCN) model, which addresses the issues of and memory contingencies in Metaverse NIDS models. The QAT model is made interpretable using eXplainable artificial intelligence (XAI) methods namely, SHapley additive exPlanations (SHAP) and local interpretable model-agnostic explanations (LIME), to provide trustworthy model transparency and interpretability. Overall, the proposed method contributes to storage benefits four times higher than the original model without quantization while attaining a high accuracy of 99.82%.**

***Index Terms*—AI, Cyber Security, IoT, Metaverse, Network, Tiny Machine Learning, XAI.**

I. INTRODUCTION

The preeminent challenges in Metaverse development today involve cultivating user trust, advancing identity management, and fortifying overall security [1]. The Metaverse refers to a simulated 3D virtual environment that offers a seamless interaction between a physical and virtual space. The widely used terms such as virtual reality (VR) and augmented reality (AR) offer a simulated virtual experience to the user while incorporating various components [2], [3] like; computation, storage, communications, artificial intelligence (AI), Blockchain, and the internet of things (IoT), as illustrated in Fig. 1. Huge interests and investments in the Metaverse market are increasing daily as its services promise to be a game-changer for the future of remote work, social interaction, and entertainment.

Alongside the substantial prospects of the Metaverse, identity management, trust, and privacy of users are becoming a key concern [1]. Metaverse security aims at the protection of Metaverse assets, users, and infrastructure from various forms of cyber risks. To satisfy the urgent demands of users, most Metaverse applications and services are being pushed to the market without enough security scrutiny, thus leaving consumers vulnerable. Various identity threats, vulnerabilities, malware, and cyberattacks have been perpetuated due to the lack of extensive security testing and the establishment of modern cyber-defense mechanisms that mitigate against diverse attack surfaces. [4].

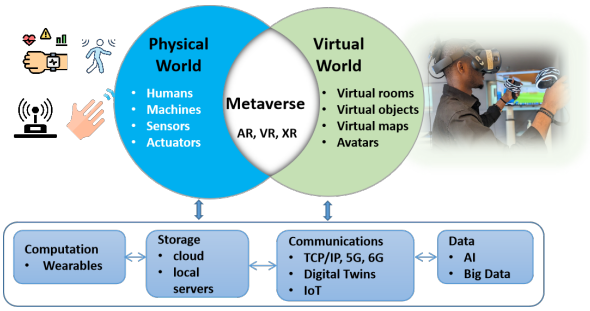

Fig. 1. Summarized concept of the Metaverse with various vital components.

As IoT-enabled haptic devices which serve as a bridge between the physical and virtual world increase [5], advanced persistent threat (APT) groups leverage the vulnerabilities of Metaverse IoT devices to perpetuate severe cyberattacks that adversely affect the cybersecurity of various IoT networks. Specifically, these hacker groups facilitate their criminal activities, by hacking IoT-based connections that transmit sensory, biometric, and location information, which is vital for achieving the augmented experience in the Metaverse. Therefore, restricting access from all kinds of suspicious or anomalous traffic has become expedient in Metaverse applications or services, where security requirements are highly critical [1].

While AI algorithms have been explored as a viable deterrent technique to reduce various cyber-risks either by monitoring, restricting access, or detecting malicious traffic [6], real-time security against cyberthreats and vulnerabilities in Metaverse networks comes at the cost of high resource requirements. Thus, the utilization of cost-efficient (Tiny) [7] machine learning (ML) solutions can increase bandwidth efficiency within Metaverse-IoT networks because most IoT devices have a high computational demand with limited energy resources. To solve the problem of high bandwidth consumption in AI models, new studies have employed the model quantization technique, in which its exclusive application may prove inadequate in the development of a quantized integer model [8]. Furthermore, re-

cent advances in AI-based NIDS model development highlight the need to provide transparency and better interpretation of AI-based NIDS models to reduce false alarm rates and provide security stakeholders with explainable AI (XAI), reliable, and strengthened security debugging policies against diverse types of IoT network traffic [7].

Motivated by the above-mentioned issues, this work proposes an efficient and explainable detection of anomalous network traffic in Metaverse networks with high security requirements (virtual-health, virtual-learning, and virtual-meetings). This study envisions an integrated framework that encompasses present-day key technologies, including NIDS model quantization and XAI interpretations, which bolsters increased reliability and security postures against network vulnerabilities in Metaverse networks.

First, proper network traffic feature selection (FS) methods (filter, wrapper, and embedded) methods) are crucial when building AI-IoT-enabled NIDS solutions. A union method of feature selection exhibits a distinctive approach to integrate and accommodate significant features that are usually overlooked by stand-alone feature selection techniques [9].

Second, there is a need to improve NIDS model detection efficiency through the use of the quantization training process, which can stimulate the model to learn quantization-friendly weights and activations more efficiently. By adopting a meticulous *'bit-by-bit' approach within the quantization-aware training (QAT)* process, model outputs can lead to better quantization results and increased cost savings for the AI-based NIDS models.

Finally, visual XAI of black box model predictions can help security experts improve security policies, model debugging, and proper hardening against security vulnerabilities from malicious traffic within IoT-enabled Metaverse networks.

The overall approach proposed in this study provides a novel framework that integrates an efficient union feature selection method with *Tiny* aware and explainable model training for trustworthy and efficient detection of cyberthreat traffic classification in the Metaverse.

This paper focuses on the following research questions (RQ):

- **RQ1**: How important is it to encode trust by preventing anomalous traffic implications in IoT-based Metaverse applications?
- **RQ2**: Since AI-based NIDS models require important features for real-time network traffic detection, how viable can the union feature selection method lead to better model performance?
- **RQ3**: How can Metaverse haptic sensors/devices with low computational constraints be made more computationally efficient with a quantization-aware training process (QAT)?
- **RQ4**: Why should we trust ML predictions in IoT-based Metaverse networks? How can NIDS models be made more qualitatively and visually interpretable?

The contributions of this study are as follows.

1) It discusses the relevance of preventing malicious traffic in IoT-enabled Metaverse networks with high-security demands.
2) It investigates the union FS method as a better approach for model features towards addressing cyber threat detection in the Metaverse.
3) It utilizes a quantization-aware training method that can address the need for cost-efficient (*Tiny*) network traffic classification, without sacrificing accuracy.
4) It provides a visual interpretation of model prediction using the SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) of anomalous from benign network traffic, to satisfy XAI demands in the Metaverse.

II. BACKGROUND AND RELATED WORKS

This section provides the security burdens of Darkwebs in the IoT and the different contemporary approaches used for detecting and categorizing its network traffic.

A. Malicious Network Traffic Detection Method.

Recent research has attempted to solve the problem of cyber-attack network traffic classification at the packet or flow level [6]. Other approaches have ignored proper feature selection techniques [10] but used a wholesome 72 remaining features after the preprocessing steps. Meanwhile, in the field of NIDS model development, dataset dimensionality and proper feature selection have also become a bottleneck for efficient NIDS.

A union FS method has been explored in [9], where the authors utilized a simple ensemble majority voting process to derive 20 optimal features. Their approach revealed that leveraging on a single FS technique may lead to the dropping of relevant features such as *flow bytes and packets*, thus resulting in potential consequences such as low detection accuracy, especially in different types of network attacks that rely heavily on flow-based features.

B. Deep Learning for Darkweb Traffic Classification

Unlike traditional ML classifiers, which are limited in their ability to extract features of massive data considering massive cyber traffic in real life, the use of neural networks for network traffic classification has been preferred by modern research [11]. Based on the published VPN-nonVPN ISCXVPN2016 dataset, increased interest in deep learning method applications for Darknet traffic classification has gained wide interest [12]. The authors in [13] proposed different ML techniques, including convolutional neural network-long short-term memory (CNN-LSTM) and convolution-gradient recurrent unit (CNN-GRU), to recognize the illegalities of darkweb network traffic using the DIDarknet dataset.

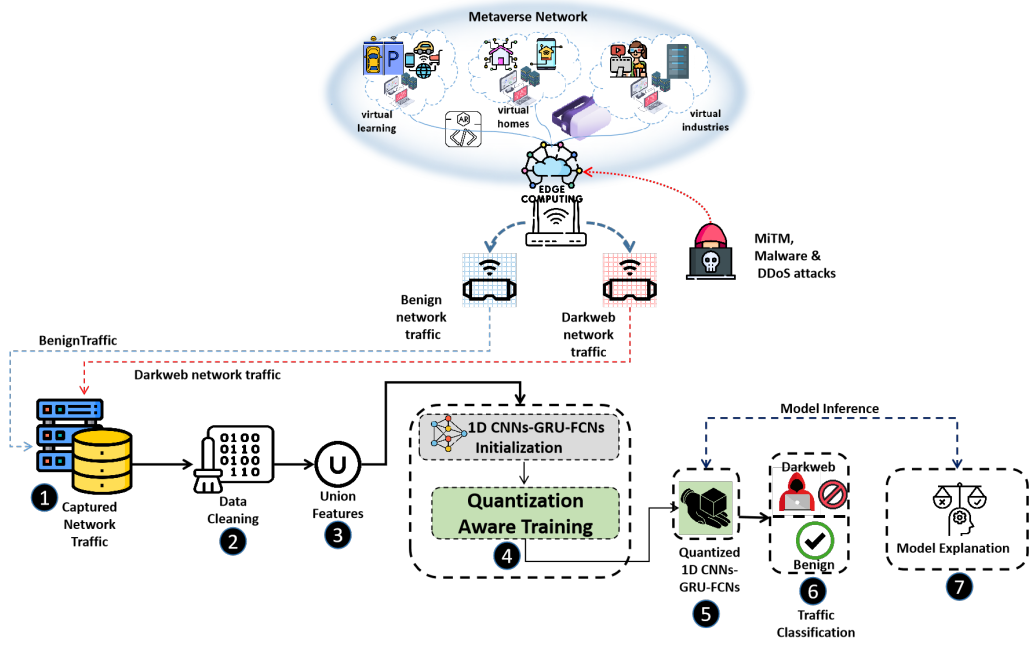

Fig. 2. The proposed approach for darkweb detection in IoT-enabled Metaverse network, integrating union feature selection, QAT, and XAI.

C. Quantization Aware Training (QAT) for Model Efficiency

To address the issue of computational overhead, compression mechanisms [14] and quantization algorithms can effectively compress the model size (memory costs) to provide *Tiny* models [7] which can reduce resource consumption.

Quantization methods can be broadly classified into post-quantization and quantization-aware training. *Quantization methods are achieved by reducing the precision bits* used to represent a model's parameters, which by default are 32-bit floating-point numbers, where model weights, activations, or gradients of both can be quantized. The authors in [15] proposed network-based quantization (low-bandwidth fixed-point format) to compress upstream and downstream data in IoT networks significantly. The results of the proposed technique yielded lightweight, locally quantized neural network training with less computational complexity and memory footprint. This study validates that the QAT method provides more control of model weights during the training process than the PQT method for NIDS efficiency.

D. NIDS Model Explanations (XAI)

To improve the trustworthiness, transparency, and reliability of AI-enabled NIDS in the Metaverse, there have been robust XAI investigations by cybersecurity experts and researchers in IoT CPSs like: *How can we trust the predictions of NIDSs ?, What specific traffic features contributed to the NIDS decisions?*

XAI is an AI-enabled NIDS that aims to understand the intrinsic model properties to prevent cyberattacks [16]. Two categories of explainability methods, *post hoc and ad hoc*, have been adopted for XAI-enabled NIDS. The ad-hoc explainability method provides model explanations during the decision process. In contrast, the post-hoc methods offer explainability information after model prediction, such as feature contributions to the model output. Commonly used post-hoc explainability methods in NIDS domains are SHAP and LIME, and various IoT cyberattacks can gain better insights and visualizations into the nature of these attacks and model explanations to perform efficient cyber threat remediation [13].

III. PROPOSED APPROACH

The proposed cross-silo NIDS model comprising quantization-aware training and XAI interpretations for classifying anomalous traffic within Metaverse CPSs is shown in Fig. 2. The proposed novel approach offers current AI-based NIDS frameworks that can solve malicious traffic detection within the Metaverse with improved model memory costs and interpretability.

First, Metaverse network traffic consisting of malicious and normal traffic is captured using traffic-capturing tools. Next, the proposed approach adopts a union FS method with viable features from the Pearson correlation coefficient (PCC) union set and decision tree (DT) algorithms. Eventually, deep learning models are employed for classification tasks due to their outstanding performance in capturing more complex traffic features in the NIDS domain [17]. Some of these include a simple deep neural network (DNN), RNN, 2D Convolutional LSTM (ConvLSTM2D), and proposed 1D CNN followed by

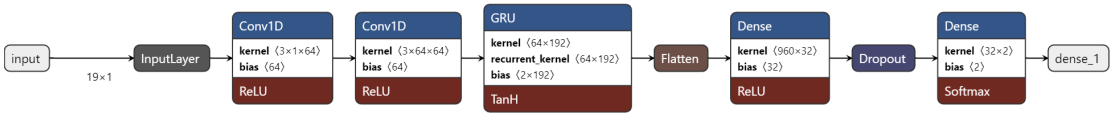

Fig. 3. illustrates the proposed 1D CNNs-GRU-FCNs model for Metaverse darkweb traffic classification.

fully connected networks (1D CNNs-GRU-FCNs) for model training and evaluation.

A. Proposed Hybrid NIDS Model (1D CNNs-GRU-FCNs)

The evaluated hybrid models leveraging a 1D CNNs-GRU-FCNs model are trained on IoT network traffic data that has been preprocessed, standardized, and encoded using one-hot encoding. The neural network architecture includes Conv1D layers, a GRU layer, and densely connected layers, as shown in Fig. 3, which effectively captures complex darkweb from benign IoT traffic.

The model was trained using an Adam optimizer (0.001) for 20 epochs to minimize the loss function while optimizing the weights and biases. The 1D CNNs-GRU-FCNs NIDS model was evaluated with QAT to make the NIDS model more memory-efficient and suitable for deployment in IoT scenarios with limited resources while preserving its accuracy, unlike less accurate/aggressive methods, such as binarization and post-training methods. The 8-bit QAT, as represented in Equation 1, is applied to each layer, thereby optimizing the model for execution on the NIDS hardware with reduced numerical precision.

$$QuantizedWeight(W_0) = Round((\frac{W_i}{S}) + \varepsilon) \times S + \delta \quad (1)$$

Where W_i is the original weight, ε denotes small bias or adjustment to the value before rounding, S is the scaling factor, and δ is the offset term that adjusts the QAT values to account for bias. Eventually, post-hoc XAI methods (SHAP and LIME), owing to their model-agnostic and real-time suitability [16] are employed to evaluate the reliability, trustworthiness, and transparency of the NIDS model's prediction of darkweb traffic.

B. Model Explainability

The SHAP explainer provides the marginal value of contributions made by a subset of features. In contrast, the LIME explainer generates local surrogate models to approximate the decision-making process of a complex model, providing interpretable explanations for individual predictions by highlighting important features. An evaluation of the explainability methods helps obtain a subjective assessment of the security expert's trust and assessments of the 1D CNNs-GRU-FCNs model's trustworthiness.

IV. EXPERIMENT AND EVALUATION

A. Dataset Selection, Preprocessing, and Simulation Setup

This work conducted systematic experiments to evaluate the 1D CNNs-GRU-FCNs NIDS model performance with and without QAT using the standard CIC-Darknet 2020 dataset [13]. The choice of this dataset is motivated by its relevance towards gaining inherent similarities in darkweb IoT-based communications and malicious TCP/IP communications in Metaverse environments [5]. The dataset is split into training and testing sets using the train-test-split Keras and Scikit-learn modules, with data samples split 80% for training and 20% split for testing.

After carefully measuring the natural cutoff points in the feature distributions, 0.8 is chosen as an appropriate threshold to select the top 10 traffic features of the DT and PCC methods using the Scikit learn Min-Max Scaling function. The PCC omits very important traffic features like the *flow duration*, while the DT includes important features dropped features by the PCC while ranking top features based on their information gain. The union feature selection complements the weakness of the PCC and DT methods and is arrived at by combining the 10 best features from the PCC and DT algorithms ($PCC \bigcup DT$) summing up to 20 viable traffic features including the target class, to perform a binary class prediction of Tor (darkweb) vs normal traffic. **The simulation was conducted** in a Python environment with the Tensorflow 2.9.0 library on a Windows 10 OS with the configuration of Intel(R) Core(TM) i3-7100 CPU @ 3.90GHz, 8GB RAM, and a Tesla K80 GPU.

B. Model Performance and Evaluation Metrics

The performance of the QAT 1D CNNs-GRU-FCNs model is evaluated adequately to the degree of correctness and model cost savings. The evaluation metrics within the experiment include the F1-Score, accuracy, test loss value, area under the curve (AUC), and model cost savings (bytes). Accuracy is the simple mean of model correctness obtained from the difference in predictions from the labeled ground truth data.

C. Result Discussion based on Research Questions

1) ***RQ1*** *:* In light of the surveyed discussions in sections I and II, it is justifiable to argue that preventing Metaverse darkweb traffic contributes to safeguarding the integrity and confidentiality of IoT networks [1], [13].

2) ***RQ2*** *:* As shown in Table I, in sufficient quantity and quality of traffic features would contribute to lesser detection accuracy; meanwhile, a union FS method yields a higher detection accuracy. **The proposed union FS method with the posited ID CNNs-GRU-FCN model shows more significant improvement in Table I, in identifying *especially Tor* and Normal network traffic**, with an 87% accuracy, and 99.83% respectively, thus addressing.

TABLE I
EXPERIMENTAL RESULTS USING THE CICDARKNET 2020 DATASET

Union	Model	Accuracy %	F1-Score %	Loss	AUC score %	Normal %	Tor %
PCC	DNN	99.49	99.43	0.0301	92.69	100	56
	ConvLSTM2D	99.49	99.42	0.0251	94.48	100	55
	RNN	99.29	99.16	0.0319	93.65	100	40
	1D CNNs-GRU-FCNs	99.54	99.5	0.0202	97.32	100	65
DT	DNN	99.65	99.64	0.0177	99.47	100	78
	ConvLSTM2D	99.57	99.73	0.0109	99.57	100	80
	RNN	99.72	99.72	0.011	99.59	100	83
	1D CNNs-GRU-FCNs	99.81	99.8	0.0074	99.83	100	85
Union	DNN	99.72	99.71	0.016	99.59	100	83
	ConvLSTM2D [18]	99.74	99.72	0.0112	99.65	100	79
	RNN [19]	99.77	99.76	0.011	99.6	100	82
	1D CNNs-GRU-FCNs	99.83	99.82	0.0074	99.82	100	87
	QAT ID CNNs-GRU-FCN	**99.83**	**99.82**	**0.0085**	**99.82**	**100**	**87**

3) ***RQ3****:* Concerning evaluating a Tiny NIDS model for Metaverse darkweb detection, the QAT method contributes to storage benefits four times better than the model without quantization. The QAT approach in Fig 4 using the QAT ID CNNs-GRU-FCN model, compared with the ordinary model without QAT, yields competitive accuracy values using the least amount of memory. Excessive memory consumption remains a big problem in the Metaverse. However, the critical takeaways between the comparison of the ID CNNs-GRU-FCN model with an accuracy of 99.83% (273544 storage bytes) and the QAT ID CNNs-GRU-FCN attaining a close 99.82% with lesser storage costs of (68386 bytes) shows that the proposed method can be integrated into IoT enabled Metaverse haptic devices to satisfy security efficiency and bandwidth utility.

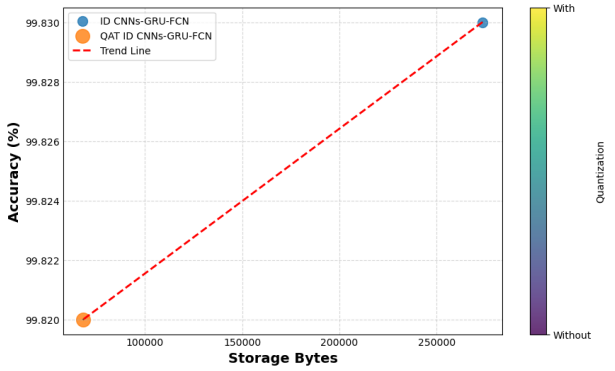

Fig. 4. Shows a storage comparison of the Original ID CNNs-GRU-FCN Model without quantization, vs the **QAT** ID CNNs-GRU-FCN Model.

4) ***RQ4:*** *Model Explainability Performance:* As shown in Fig. 5, DeepSHAP feature importance plot based on a few subsets of test data enables a network expert or user with basic visualization skills to investigate the most contributing network traffic feature(s) *(Fwd Seg Size Min ...)* that led to the QAT ID CNNs-GRU-FCN model's prediction. Thus providing XAI insights like model debugging, feature selection, feature engineering, and more precise explanations *(of what features led to this prediction?) and satisfy XAI demands in the Metaverse*.

Fig. 6 specifically interprets and measures the probability of the model prediction within subset traffic to ascertain if

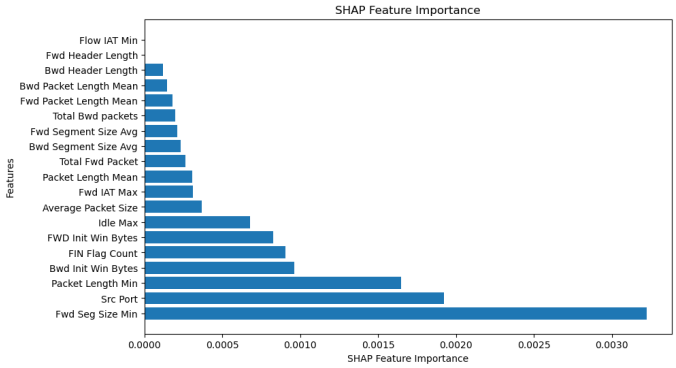

Fig. 5. shows the SHAP feature importance of the QAT ID CNNs-GRU-FCN model.

darkweb or benign using the LIME explainability method. As shown in Fig. 6, the LIME explainer is 100% certain that the network traffic is benign and not darkweb traffic.

In summary, Table II shows that the proposed approach outperformed contemporary approaches.

TABLE II
PRESENTATION OF THE PROPOSED FRAMEWORK WITH SOTA DARKWEB CLASSIFICATION METHODS.

Author	Model	Dataset	Acc.%	Tiny ML	XAI
[13]	CNN-LSTM	Darknet	96	×	×
[13]	MLP	NSLKDD	79	×	✓
[7]	DT	MNIST	91.5	✓	×
Ours	ID CNNs-GRU-FCN	Darknet	99.82	✓	✓

V. CONCLUSION

This study developed a tiny (QAT) and explainable framework for darkweb detection in IoT networks. A hybrid (1D CNNs-GRU-FCN) model with a union FS method was used to effectively identify dark web traffic, achieving a strong model performance. Through quantization-aware training, we address the cost issues of the NIDS model (fourfold improvement) while maintaining a balance between accuracy in resource-demanding IoT scenarios. To enhance the XAI model for security experts, we integrated visually interpretable and quantitative (XAI) methods such as SHAP and LIME. Future

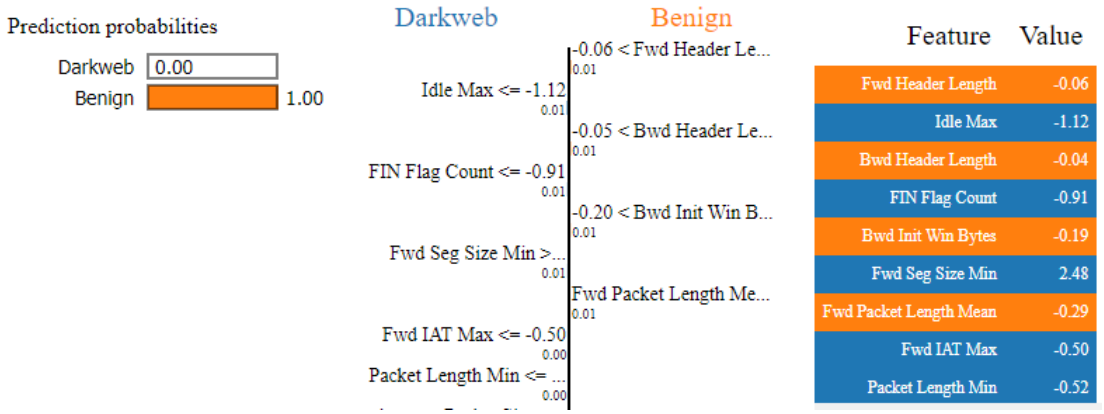

Fig. 6. shows the LIME probability prediction of the QAT ID CNNs-GRU-FCN model.

work will address other computational costs of the proposed framework.

ACKNOWLEDGMENT

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(MEST)(2018R1A6A1A03024003) & Ministry of Science and ICT, Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation).

REFERENCES

[1] M. Choi, A. E. Azzaoui, S. K. Singh, M. M. Salim, S. R. Jeremiah, and J. H. Park, "The Future of Metaverse: Security Issues, Requirements, and Solutions," *Human-Centric Computing and Information Sciences*, vol. 12, no. 60, 2022. [Online]. Available: http://hcisj.com/articles/?HCIS202212060

[2] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D.-S. Kim, "Prospects and challenges of metaverse application in data-driven intelligent transportation systems," *IET Intelligent Transport Systems*, vol. 17, no. 1, pp. 1–21, 2023.

[3] J. N. Njoku, C. Ifeanyi Nwakanma, and D.-S. Kim, "The role of 5g wireless communication system in the metaverse," in *2022 27th Asia Pacific Conference on Communications (APCC)*, 2022, pp. 290–294.

[4] M. Vondrek, I. Baggili, P. Casey, and M. Mekni, "Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses," *Computers & Security*, vol. 127, no. 102923, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822003157

[5] V. T. Truong and L. B. Le, "Metacids: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 253–266, 2023.

[6] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Shap-based intrusion detection framework for zero-trust iot maritime security," in *2023 The 2nd International Conference on Maritime IT Convergence (ICMIC)*, 2023, pp. 1–8. [Online]. Available: https://www.researchgate.net/publication/373489659_SHAP-Based_Intrusion_Detection_Framework_for_Zero-Trust_IoT_Maritime_Security

[7] S. A. R. Zaidi, A. M. Hayajneh, M. Hafeez, and Q. Z. Ahmed, "Unlocking edge intelligence through tiny machine learning (tinyml)," *IEEE Access*, vol. 10, pp. 100 867–100 877, 2022.

[8] C.-C. Chung, W.-T. Chen, and Y.-C. Chang, "Using quantization-aware training technique with post-training fine-tuning quantization to implement a mobilenet hardware accelerator," in *2020 Indo – Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN)*, 2020, pp. 28–32.

[9] S. Das, S. Saha, A. T. Priyoti, E. K. Roy, F. T. Sheldon, A. Haque, and S. Shiva, "Network intrusion detection and comparative analysis using ensemble machine learning and feature selection," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4821–4833, 2022.

[10] N. Rust-Nguyen, S. Sharma, and M. Stamp, "Darknet traffic classification and adversarial attacks using machine learning," *Computers and Security*, vol. 127, p. 103098, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823000081

[11] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Cyber-chameleon: A moving target defence mechanism for metaverse cyberattacks," *The 2023 Korean Institute of Communication Science Fall Conference*, pp. 49–50, 2023. [Online]. Available: https://www.researchgate.net/publication/376035110_Cyber-Chameleon_A_Moving_Target_Defence_Mechanism_for_Metaverse_Cyberattacks

[12] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and vpn traffic using time-related," in *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, 2016, pp. 407–414.

[13] K. Sauka, G.-Y. Shin, D.-W. Kim, and M.-M. Han, "Adversarial robust and explainable network intrusion detection systems based on deep learning," *Applied Sciences*, vol. 12, no. 13, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/13/6451

[14] H. Yang, L. Duan, Y. Chen, and H. Li, "Bsq: Exploring bit-level sparsity for mixed-precision neural network quantization," *arXiv preprint arXiv:2102.10462*, 2021.

[15] Y. Ji and L. Chen, "Fedqnn: A computation–communication-efficient federated learning framework for iot with low-bitwidth neural network quantization," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2494–2507, 2023.

[16] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable artificial intelligence in cybersecurity: A survey," *IEEE Access*, vol. 10, pp. 93 575–93 600, 2022.

[17] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *2016 8th IEEE international conference on communication software and networks (ICCSN)*. IEEE, 2016, pp. 581–585.

[18] I. Ullah and Q. H. Mahmoud, "Design and development of rnn anomaly detection model for iot networks," *IEEE Access*, vol. 10, pp. 62 722–62 750, 2022.

[19] M. B. Sarwar, M. K. Hanif, R. Talib, M. Younas, and M. U. Sarwar, "Darkdetect: Darknet traffic detection and categorization using modified convolution-long short-term memory," *IEEE Access*, vol. 9, pp. 113 705–113 713, 2021.