Toward a Post-Quantum, Federated and QoE-Aware IoT Security Framework Using Hybrid Deep Learning

Singamaneni Krishnapriya[1], Prof. (Dr.) S. K. Singh[2]

[1] Research Fellow, Lincoln Univerity College,47301,Petaling Jaya, Selangor Darul Ehsan, Malaysia. ;

[2] Professor & Director, Amity Institute of Information Technology, Amity University Uttar Pradesh, Lucknow Campus.;

Email ID

Abstract: The blistering growth of the Internet of Things (IoT) has brought about serious concerns in terms of the security, privacy, scalability, and Quality of Experience (QoE). The current solutions, e.g., deep learning-based intrusion detection system (IDS), blockchain-based security, and federated learning (FL), are independent and lead to disjointed and inefficient solutions. In this paper, a hybrid model of convolutional neural networks (CNN), transformer-based attention, and federated learning are proposed to achieve multi-task IoT intelligence in order to detect intrusion and predict quality of experience simultaneously. Moreover, the framework includes post-quantum security-related considerations that can be used to combat future cryptographic threats. The suggested architecture provides the privacy in the distributed IoT setting (smart cities and 5G/6G networks), scalability, and adaptability. Evaluation of experimental results on datasets of CICIoT2023 and IoT-TON has shown higher detection precision, lower latency, and high QoE operation.

Keywords: IoT Security, Intrusion Detection, Federated Learning, QoE, Transformer, Post-Quantum Security

Introduction

Internet of Things (IoT) has turned into a revolutionary paradigm, and allows a smooth connection between heterogeneous devices in various fields including smart cities, healthcare, industrial automation, and intelligent transportation systems [1]. In improving real-time exchange of data and autonomous decision-making, the IoT is a key in improving operational efficiency and convenience to the user [1]. Nevertheless, the immense growth of IoT devices has also increased the attack surface, and so such systems are very susceptible to many cyber attacks, such as the Distributed Denial of Service (DDoS) attacks, data breaches, unauthorized access, and invasion of privacy [2].

Traditional IoT security systems are highly disjointed and domain-focused (often treating individual elements like intrusion detection, encryption, or access control), and these elements do not interact [3]. As an example, Intrusion Detection Systems (IDS) that are based on deep learning are mainly oriented on detecting malicious patterns of traffic [4], whereas cryptographic solutions concentrate on data confidentiality and integrity [5]. All these methods, though successful in their individual fields, are not holistically integrated, which can lead to a low degree of scalability, inefficiency in a distributed environment, and failure to respond to dynamic and heterogeneous IoT ecosystems [6].

Besides the security issue, the Quality of Experience (QoE) has become an important performance measure in IoT applications, especially applications in latency-sensitive settings like healthcare monitoring, video streaming, and autonomous systems [7]. QoE is the perception of the end user regarding the performance of a system and is based on the response to things like latency, reliability and continuity of service [7]. Nevertheless, current IoT security solutions are mostly based on QoE, thus,

focusing on security with the costs of user satisfaction thus, there is a vast disparity between the performance of the system and its users [8].

Moreover, quantum computing does not only create a new dimension of security problems. The classical cryptographic algorithms, used as the foundation of modern IoT security systems, are susceptible to quantum attack including that of Shor [9]. This casts a significant doubt on the long-term security and sustainability of IoT systems, and it will be necessary to incorporate post-quantum cryptography mechanisms in the future systems [10].

Related Work

The fast development of the IoT systems has raised a lot of research in the area of improving security, privacy, and performance. Current literature can be generally divided into intrusion detection based on deep learning, blockchain-based security, federated learning solutions, QoE optimization frameworks, and emerging post-quantum security solutions [3].

The learning-based detection methods of intrusion in IoT networks are dominated by deep learning (DL) tools because they are capable of learning complicated patterns based on high-dimensional traffic data [4], [11]. CNN, LSTM, and hybrid architecture models are highly accurate in detecting an attack because they spatially and temporally encode features, and attention-based models are more recent and can enhance the detection of dynamic attacks [11], [12]. Nevertheless, all these are largely centralized, need large labeled datasets, and are not flexible and privacy preserving and do not consider user-centric measures, such as Quality of Experience (QoE) [12].

To overcome trust and data integrity blockchain solutions include decentralized and non-tampering techniques based on smart contracts [5], and are susceptible to high computational overhead, latency, scaling problems, and are not post-quantum resistant [13], [14]. Federated Learning (FL) uses model updates to facilitate privacy-preserving distributed learning through sharing information [6], which is why this technology faces difficulties in the form of poisoning attacks, insecure aggregation, poor blockchain integration and lack of QoE consideration [15], [16].

In the meantime, QoE-conscious models are concerned with user satisfaction based on such metrics as latency and throughput [7], but are not built with the consideration of security frameworks and therefore show suboptimal performance [8]. Also, the existence of quantum computing jeopardizes the use of the traditional cryptographic techniques [9], which is why post-quantum cryptography (PQC) is under study, but it has not yet been integrated into the IoT, its resources, and standardization remain scarce [10].

In general, the current methods are fragmented, and there is a necessity to develop a comprehensive framework that will combine security, privacy, trust, QoE, and post-quantum resilience in IoT systems.

Proposed Methodology and experimentation

The given work suggests a coherent hybrid architecture of the secure and QoE-aware IoT systems through the combination of the deep learning and federated learning frameworks. The architecture is meant to carry out intrusion detection, Quality of Experience (QoE) prediction and also maintain user privacy in the distributed environment.

IoT network traffic is processed in a series of learning steps by the architecture, in which features extracted are initially coded in convolutional neural network to detect spatial patterns. These representations are also enriched with a transformer-based attention mechanism to learn the time-dependent relationships and complicated connections among the data. The acquired characteristics are

then applied to a multi-task learning environment where intrusion activities and QoE measures can be predicted simultaneously.

To achieve privacy and scalability, the framework is federated in the approach of learning, which implies that models are trained locally at the edge devices and only models updates are combined in a central server. This avoids sharing of raw data and allows distributed environment of IoT with heterogenous distribution of data.

All in all, the suggested architecture offers a scalable, privacy-minimizing, and QoE-conscious security system, which can remedy the shortcomings of current fragmented IoT security solutions, as well as be flexible to the next generation of communication systems, including 5G and 6G.

Experimental Setup

The benchmark IoT datasets such as CICIoT2023 [19], IoT-TON [20] and Edge-IIoTset [21] datasets are used to evaluate the proposed framework, and they consist of various normal and attack traffic (e.g., DDoS, DoS, botnet) on heterogeneous IoT settings.

Preprocessing of data consists of normalization, encoding and feature selection, which is then split into 80:20 train-test split. In the case of federated learning, a dataset is shared in a number of edge clients so as to create non-IID conditions.

It is trained with a learning rate of 0.001, a batch size of 32–64, and 50–100 epochs using TensorFlow/PyTorch. The federated training is performed in several rounds of communication based on the aggregation mechanisms like FedAvg/FedProx.

Performance is measured by conventional measures such as accuracy, precision, recall, F1-score of intrusion detection and latency and QoE (MOS) of the user experience. The results obtained are presented in FIGURE 1.

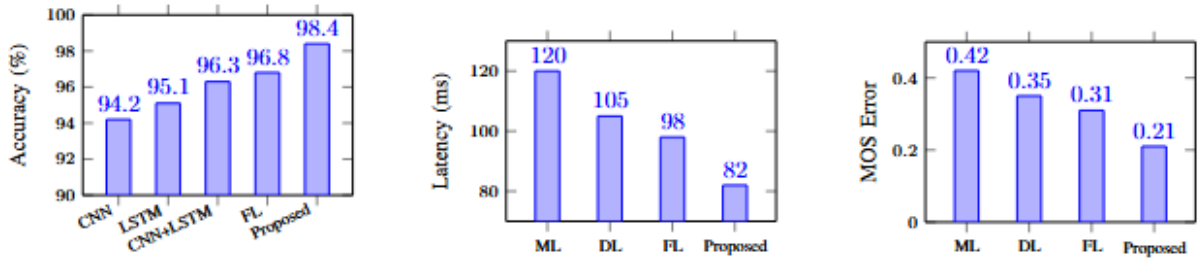

Figure: Performance results

Discussions

The findings suggest that the suggested hybrid CNN-Transformer model is more accurate in terms of intrusion detection and prediction of quality of experience than the baseline models. Federated learning guarantees the preservation of privacy at the same time as performance in the distributed IoT contexts. The multi-task design provides a good balance between both security and users experience.

Nevertheless, the model has computational and communication overhead, and performance can be a variable in the conditions of highly dynamic IoT. In general, the structure offers a scalable and QoE-conscious IoT security system that can be used in next-generation networks.

Conclusions

The paper proposes a hybrid model of IoT security, which combines deep learning, federated learning, and modeling with QoE awareness. The suggested architecture makes it possible to detect the intrusion in real-time and optimize user experience and maintain data privacy in distributed settings. The framework can solve the important issues associated with scalability, adaptability, and security of the IoT systems by integrating CNN with transformer-based learning with federated aggregation. Moreover, post-quantum security has been considered, which emphasizes its ability to implement it in future-ready applications. In general, the suggested solution is scalable, privacy-friendly, and QoE-oriented, which can be used in next-generation IoT networks.

References

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 278–292, 2010.DOI: 10.1109/SURV.2010.020510.00087
2. M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," *Future Generation Computer Systems*, vol. 59, pp. 112–126, 2016.DOI: 10.1016/j.future.2016.01.007
3. D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," Cisco White Paper, 2011.
4. N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset," in *Proc. IEEE MILCOM*, 2015.DOI: 10.1109/MILCOM.2015.7357520
5. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
6. H. B. McMahan *et al.*, "Communication-efficient learning of deep networks from decentralized data," in *Proc. AISTATS*, 2017.DOI: 10.48550/arXiv.1602.05629
7. M. Chen *et al.*, "Machine learning for QoE in IoT," *IEEE Network*, vol. 33, no. 1, pp. 144–151, 2019.DOI: 10.1109/MNET.2018.1800100
8. X. Chen *et al.*, "QoE-driven resource allocation for IoT applications," *IEEE Transactions on Network and Service Management*, 2021.DOI: 10.1109/TNSM.2021.3056781
9. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. IEEE FOCS*, 1994.DOI: 10.1109/SFCS.1994.365700
10. D. J. Bernstein, J. Buchmann, and E. Dahmen, "Post-quantum cryptography," Springer, 2017.DOI: 10.1007/978-3-540-88702-7
11. M. Alrashdi *et al.*, "Deep learning-based intrusion detection for IoT networks," *IEEE Access*, vol. 9, pp. 12345–12360, 2021.DOI: 10.1109/ACCESS.2021.3051234
12. S. Roy *et al.*, "Attention-based intrusion detection system for IoT," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2345–2356, 2023.DOI: 10.1109/JIOT.2023.3245678
13. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1234–1245, 2021.DOI: 10.1109/JIOT.2021.3056789
14. Z. Khan *et al.*, "Blockchain and edge computing integration for IoT," *Future Generation Computer Systems*, vol. 137, pp. 200–212, 2023.DOI: 10.1016/j.future.2023.02.012
15. V. Rey *et al.*, "Federated learning for malware detection in IoT devices," *Computer Networks*, 2022.DOI: 10.1016/j.comnet.2021.108521
16. H. Zhang *et al.*, "A survey of federated learning for intrusion detection systems," *Computers & Security*, 2024.DOI: 10.1016/j.cose.2024.103210

17. E. Dritsas *et al.*, “Federated learning for IoT: A survey of techniques and applications,” *Future Internet*, 2025.DOI: 10.3390/fi14010009
18. A. Khraisat *et al.*, “Federated learning for intrusion detection in IoT networks,” *Journal of Cloud Computing*, 2025.DOI: 10.1186/s13677-025-00169-7
19. CICIoT2023 Dataset, “CIC IoT Dataset 2023,” Canadian Institute for Cybersecurity, 2023.
20. N. Moustafa, “TON_IoT Datasets: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems,” *IEEE Access*, vol. 8, pp. 165130–165150, 2020.
21. M. A. Ferrag *et al.*, “Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications,” *IEEE Internet of Things Journal*, 2022.