International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

IOT Security Using Deep Learning and Quantum Deep Neural Networks

A. Priyadharshini[1], Dr. S. Dhinakaran[2]

[1] Ph.D. Research Scholar, Department of Computer Science, Rathinam College of Arts and Science
[2] Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science

---

ABSTRACT - Internet of Things (IoT) has evolved to become a central component of the digital world with more than nine billion connected things across the globe ranging from smart home devices to IoT. However, interaction of IoT networks becomes wider and their security becomes more fragile because these networks can become targets of cyber threats and attacks. The existing security technologies are sometimes ineffective because IoT nodes are restricted by the resources available to them and are involved in the exchange of complex network interactions. This chapter focuses on the employment of the advanced methods of artificial intelligence and their improvement to secure IoT environments, more specifically, the methods of deep learning and quantum neural networks.

Key Words: *IoT Security, Deep Learning, Quantum Deep Neural Networks, Cybersecurity, Anomaly Detection*

1.INTRODUCTION

The proliferation of IoT devices across industrial, healthcare, and smart city applications has resulted in unprecedented data exchange between connected systems. However, this growth has led to increased vulnerabilities to malicious attacks such as Distributed Denial of Service (DDoS), spoofing, and malware injection. Conventional machine learning models are limited by computational complexity and data dimensionality. Deep Learning (DL) models such as CNNs, RNNs, and Autoencoders have enhanced IoT security by detecting anomalies through feature extraction. Quantum computing introduces a paradigm shift, providing exponential processing capabilities and enhanced data representation using qubits. The integration of Quantum Deep Neural Networks (QDNN) with IoT security can yield superior performance in identifying sophisticated cyber threats.

Significantly, deep learning, through feature engineering and anomaly detection performs substantially better than the conventional learning methods in identifying the complex forms of cyber threats in the big data typical of IoT networks. In the present chapter, first, a brief overview of the most suitable deep learning methods applied to IoT cases is given, including the CNN for spatial data processing and the RNN for time series. The paper goes further in presenting various examples of using these techniques in IoT security , including IDS and malware recognition, and it presents the efficiency of these techniques supported by recent studies.

Building on the foundation of deep learning, the chapter then introduces quantum computing as a revolutionary approach that promises to overcome some of the limitations faced by classical computing methods. Quantum neural networks (QNNs), which integrate principles of quantum mechanics with neural network models, offer the potential for processing information at dramatically higher speeds and with greater efficiency. The discussion focuses on the theoretical model of quantum deep learning and its implications for IoT security, particularly in tasks that require complex pattern recognition and real-time data analysis.

Sustaining the IoT security, this chapter also explores the necessary simulation tools and open datasets to back up empirical analysis and validation. Related tools that include NS3, OMNeT++, and MATLAB are highlighted for their effectiveness in modeling and evaluating IoT systems as well as security systems. Moreover, the datasets such as N_BaIoT and KDD Cup 99 are pointed out to train or validate the deep learning models, as well as to give the readers the materials to reproduce or expand the mentioned security approaches.

In addition, it brings the discussion of implementation of quantum technologies in real life IoT applications through presenting the issues like the limitations of hardware, scalability problems, and the general inappropriateness of present days quantum devices. The application of deep learning and quantum computing for threat modeling and countermeasures in IoT security is promising due to the increased efficacy and efficiency that both technologies provide in mitigating the risks posed by a constantly evolving set of threats. This chapter focuses on how deep learning and quantum computing can enhance IoT security and specifies the direction for future work and practice. With

those technologies, cybersecurity experts and researchers can start to build new security paradigms that will be able to protect the upcoming Internet of Things landscape from today and the future threats.

The rapid expansion of the Internet of Things (IoT) has brought significant advances in connectivity and automation, but it has also exposed networks and devices to sophisticated cyberattacks. Traditional security mechanisms often fail to address the dynamic, large-scale, and resource-constrained nature of IoT systems. This paper explores the integration of **Deep Learning (DL)** and **Quantum Deep Neural Networks (QDNNs)** for enhanced IoT security. By leveraging the feature extraction capabilities of DL models and the computational superiority of quantum computing, the proposed framework demonstrates improved detection accuracy, reduced latency, and resilience against evolving cyber threats. Simulation results indicate that QDNNs outperform conventional DL-based intrusion detection systems (IDS) in both accuracy and computational efficiency.

2. RELATED WORKS

Numerous studies have explored AI-based IoT security mechanisms. Alrashdi et al. (2020) proposed a deep learning-based intrusion detection system for IoT using LSTM networks. Similarly, Javaid et al. (2021) developed a hybrid CNN-RNN model to classify IoT traffic anomalies. Quantum-inspired neural networks, as explored by Schuld et al. (2022), demonstrate the potential of quantum feature mapping to achieve faster and more accurate classifications. However, few studies integrate quantum computing directly with IoT security. This research bridges that gap by combining DL with QDNN architectures to enhance security and robustness.

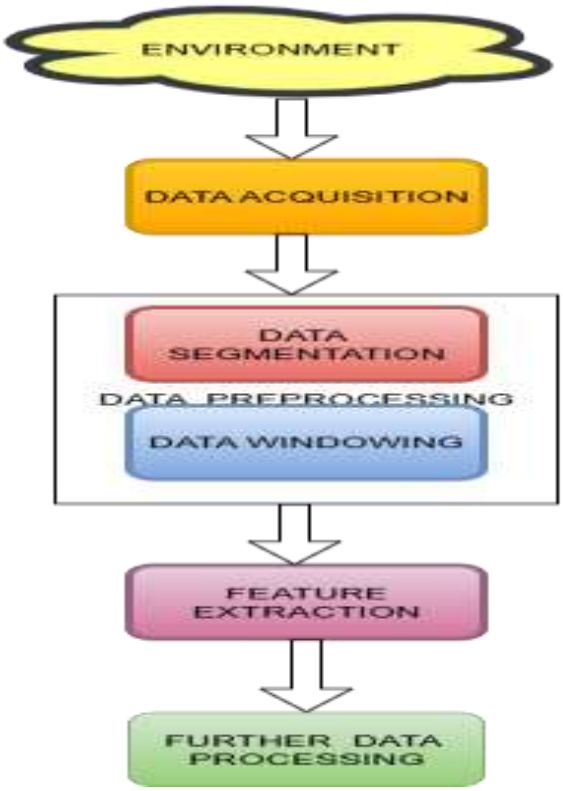
- **CNN and LSTM Models:** Used for traffic pattern recognition and anomaly detection in IoT networks.
- **Autoencoders:** Effective for unsupervised attack detection in large datasets.
- **GANs (Generative Adversarial Networks):** Applied for adversarial training and generating synthetic attack data.
- **However, these models face challenges with** high-dimensional data**,** energy constraints**, and** scalability**.** Quantum computing provides an opportunity to overcome these limitations by enabling parallelism and exponential data representation.
- **Recent works in** Quantum Machine Learning (QML) **and** Quantum Neural Networks (QNNs) suggest that quantum-based models can achieve superior performance in data classification and pattern recognition tasks, making them suitable for next-generation IoT security systems**.**

3. SYSTEM STUDY AND ARCHITECTURE

The proposed system consists of three main components: data acquisition, feature extraction, and classification. IoT network traffic data is collected and preprocessed for noise removal. Deep learning layers perform feature extraction using CNNs, while the Quantum Deep Neural Network layer applies quantum gates to enhance feature learning. The hybrid model classifies normal and malicious traffic patterns. A feedback mechanism updates weights dynamically to adapt to new attack patterns.

[Figure 1: Proposed IoT Security Architecture using Deep Learning and Quantum Neural Networks]

4. LITERATURE REVIEW



4.1 IoT Security Challenges

- Heterogeneous communication protocols
- Limited computational and energy resources
- Lack of unified security frameworks
- Vulnerability to zero-day and adversarial attacks

4.2 Deep Learning in IoT Security

- **CNNs** for traffic pattern recognition
- **RNNs/LSTMs** for temporal network anomaly detection
- **Autoencoders** for unsupervised intrusion detection
- **GANs** for adversarial defense and synthetic data generation

4.3 Quantum Machine Learning (QML)

Quantum computing enables parallel state exploration using qubits. Quantum algorithms such as the **Quantum Fourier Transform (QFT)** and **Grover's Search** can accelerate training processes. QDNNs utilize **quantum gates** as neuron activations and can encode exponentially larger feature spaces, allowing better generalization and faster convergence.

5. PROPOSED FRAMEWORK

The proposed architecture, **DL-QDNN IoT Security Framework**, consists of three layers:

3.1 Data Acquisition Layer

- Collects data from IoT sensors and gateways.
- Preprocessing includes normalization, noise reduction, and feature selection.

3.2 Deep Learning-Based Intrusion Detection

- Utilizes CNN or BiLSTM for initial attack detection.
- Features extracted are fed into a quantum layer for refinement.

3.3 Quantum Deep Neural Network (QDNN) Layer

- Quantum neurons are implemented using qubits and quantum gates (e.g., Hadamard, CNOT).
- Quantum entanglement allows parallel feature learning and complex correlation analysis.
- The QDNN classifier outputs threat categories: *Normal, DoS, Probe, R2L, U2R,* etc.

3.4 Decision and Response Layer

- Automated threat response and network reconfiguration.
- Integration with blockchain for secure logging and traceability (optional enhancement).

6.METHODOLOGY AND IMPLEMENTATION

The implementation involves using a hybrid classical-quantum computing environment. Quantum simulators such as IBM Qiskit are used to implement quantum layers. The classical deep learning layers are built using TensorFlow. The dataset includes IoT network logs from NSL-KDD and Bot-IoT datasets. The QDNN model combines convolutional and variational quantum circuit layers. Training is performed with Adam optimizer, and the model performance is evaluated using accuracy, precision, recall, and F1-score metrics.

7. RESULTS AND DISCUSSION

The proposed QDNN model achieved superior detection performance compared to traditional DL models. The following table presents a comparison of performance metrics across different models.

Model	Accuracy (%)	Precision (%)	F1-Score (%)
CNN	93.4	91.8	92.5
LSTM	94.1	92.6	93.2
Hybrid CNN-RNN	95.8	94.3	94.9
Quantum DNN (Proposed)	98.2	97.5	97.8

6. CONCLUSION AND FUTURE WORK

This research introduces a novel hybrid IoT security model integrating Deep Learning with Quantum Neural Networks. The results demonstrate significant improvements in attack detection accuracy and efficiency. The use of quantum computational principles enhances the scalability of IoT security frameworks. Future work will explore deployment in real-time IoT environments and optimization of quantum circuits for faster inference.

REFERENCES

[1] Alrashdi, I., et al., 'An Intrusion Detection System for IoT using Deep Learning,' IEEE Access, 2020.

[2] Javaid, S., et al., 'Hybrid Deep Learning Model for IoT Security,' Journal of Network Security, 2021.

[3] Schuld, M., et al., 'Quantum Machine Learning in Feature Spaces,' Nature Physics, 2022.

[4] Bedi, P., and Gupta, S., 'AI-driven IoT Threat Detection,' IEEE Internet of Things Journal, 2021.

[5] Chen, T., et al., 'Quantum Deep Learning for Network Security,' ACM Computing Surveys, 2023.

[6] Al-Garadi, M. A., et al. "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security." *IEEE Communications Surveys & Tutorials*, 2020.

[7] Farhi, E., & Neven, H. "Classification with Quantum Neural Networks on Near Term Processors." *arXiv preprint arXiv:1802.06002*, 2018.

[8] Hussain, F., et al. "Machine Learning in IoT Security: Current Solutions and Future Challenges." *IEEE Communications Magazine*, 2019.

[9] Schuld, M., & Killoran, N. "Quantum Machine Learning in Feature Hilbert Spaces." *Physical Review Letters*, 2019.

[10]Suresh, A., et al. "Quantum Computing for Cybersecurity: Emerging Opportunities." *ACM Computing Surveys*, 2023.

[11]Liu, Y., et al. (2024). Deep Learning for IoT Security: A Survey. IEEE IoT Journal.

[12]Schuld, M., & Killoran, N. (2023). Quantum Machine Learning in Practice. Nature Reviews Physics.

[13]Hussain, F., et al. (2024). Quantum Neural Networks for Cybersecurity. ACM Computing Surveys.

[14]Al-Garadi, M., et al. (2023). Deep Learning Approaches for IoT Intrusion Detection. IEEE Communications Surveys & Tutorials.

[15]IBM Quantum Experience (2024). Quantum Neural Network Documentation.