Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 6, December 2026, pp. 5371~5381
ISSN: 2302-9285, DOI: 10.11591/eei.v15i6.12530

Intelligent detection of adversaries in quantum key distribution-secured IoT networks using machine learning techniques

Dipanwita Debnath[1], Karri Manoz Kumar Reddy[2], Saka Satya Sudha[3], Anuradha Konidena[4], Vuppuloori Ravi Sekhara Reddy[5], Nallathambi Srija[6]
[1]Department of Computer Science and Engineering (AI and ML), B V Raju Institute of Technology, Narsapur, India
[2]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, India
[3]Department of Computer Science and Engineering, CVR College of Engineering, Ibrahimpatnam, India
[4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[5]Department of Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, India
[6]Department of Information Technology, M. Kumarasamy College of Engineering, Karur, India

Article Info

Article history:

Received Feb 10, 2026
Revised Sep 18, 2026
Accepted Oct 4, 2026

Keywords:

Attacker detection
Deep learning
Internet of things
Machine learning
Quantum key distribution
Railway systems

ABSTRACT

The increasing deployment of internet of things (IoT) devices in beyond-fifth-generation (B5G) and sixth-generation (6G) networks introduces significant security challenges due to limited computational and energy resources. Quantum key distribution (QKD) enables secure key establishment; however, malicious interference can compromise key generation and disrupt communication. This study aims to develop a machine learning (ML)-based framework for detecting adversarial interference using final quantum key length without interrupting QKD operation. A hierarchical architecture is proposed, assigning QKD and ML processing to capable IoT controllers and servers while maintaining lightweight sensor operations. A dataset containing 20,000 simulated QKD key-length samples, representing attack-free and attack-affected scenarios, is used to train and evaluate artificial neural network (ANN) and long short-term memory (LSTM) models. Experimental results demonstrate detection performance close to 99%, with ANN achieving substantially lower computational cost than LSTM. The framework is further considered for railway IoT monitoring, integrating fiber-optic QKD links between controllers and a control center with encrypted wireless sensor communication. The findings highlight the potential of final-key-length-based learning for lightweight, non-intrusive attack detection, while identifying synthetic data and single-feature learning as limitations requiring further validation.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Karri Manoz Kumar Reddy
Department of Electrical and Electronics Engineering, Aditya University
Surampalem, Andhra Pradesh, India
Email: kmkreddyy@gmail.com

1. INTRODUCTION

The rapid evolution of beyond-5G and 6G wireless communication is accelerating internet of things (IoT) deployment in healthcare, smart transportation, industrial automation, environmental monitoring, and critical infrastructure, while simultaneously increasing security challenges caused by resource-constrained devices and sophisticated cyber-physical attacks [1]–[3]. The limited processing, memory, and energy capabilities of IoT nodes make computationally intensive security mechanisms difficult to deploy directly, particularly in large heterogeneous networks. The emergence of quantum computing further threatens

conventional cryptographic schemes that depend on computational hardness, motivating security approaches that do not rely solely on such assumptions [4]. Quantum key distribution (QKD) provides a promising alternative because it enables two legitimate parties to establish symmetric keys while making eavesdropping detectable through quantum-state disturbances [5]. Nevertheless, practical QKD systems face hardware complexity and implementation-level vulnerabilities that may allow sophisticated attacks without necessarily exceeding conventional error thresholds [6]. A hierarchical architecture, in which QKD is performed between resource-rich servers, controllers, or gateways while constrained IoT sensors use conventionally distributed keys derived from quantum-generated material, can reduce device-level computational and energy requirements [7]. However, an attack on the QKD link between a controller and server can compromise the security of associated IoT devices. Traditional verification methods based on error-rate evaluation and test-bit comparison may require key discarding or redistribution, increasing latency and communication disruption in time-critical applications [8]. Moreover, dynamic IoT environments experience changing channel conditions, interference, and mobility, making it difficult for fixed thresholds to distinguish legitimate variations from subtle adversarial behavior. Machine learning (ML) and deep learning (DL) offer adaptive alternatives because they can identify nonlinear patterns and anomalies without requiring complete explicit models of attacker behavior [9]. Existing ML-based quantum communication studies have mainly considered physical-layer information, such as optical spectra and signal characteristics, which can require additional sensing hardware and preprocessing [10]. In contrast, this study considers statistical information generated directly during QKD, particularly the final key length after sifting and reconciliation. Changes in final key length can reflect channel noise, system imperfections, and adversarial interference, allowing attacker detection without direct quantum-state measurement or interruption of the QKD process. The proposed framework therefore investigates eavesdropping and man-in-the-middle attack detection using a baseline non-learning method together with artificial neural network (ANN) and DL approaches trained on statistically generated secure and adversarial QKD data, with a railway IoT monitoring scenario used to demonstrate potential applicability in a safety-critical environment.

Research on IoT security has addressed lightweight protection mechanisms for resource-constrained devices, while the increasing threat of quantum computing has encouraged investigations into post-quantum cryptographic approaches, including lattice- and code-based techniques [11], [12]. Although these methods can provide quantum resistance, their computational requirements and larger key sizes may create additional challenges for low-power IoT devices. QKD has consequently been investigated for modern communication and IoT infrastructures, particularly through hybrid architectures combining quantum and classical communication channels [13]. Hierarchical QKD models further reduce deployment complexity by placing quantum communication at controllers or gateways and using classical mechanisms to distribute derived keys to connected sensors [14]. Studies of practical QKD implementations have also identified vulnerabilities arising from device imperfections and channel characteristics, including attacks against continuous-variable QKD that may not activate conventional error-rate alarms [15]. ML has subsequently been applied to quantum security for detecting wavelength-dependent attacks and abnormal optical spectra, demonstrating promising detection capability under controlled conditions [16]. Other studies have used ML for QKD protocol selection and parameter optimization according to channel conditions and system performance [17]–[20], while recurrent and long short-term memory (LSTM) models have been investigated for sequential quantum measurement data and anomaly detection [21]–[25]. However, deep models generally require greater computational resources and larger datasets. Shallow ANN, in comparison, have demonstrated that low-dimensional feature spaces can often be handled with comparable detection performance while reducing training time and computational complexity [26]. Despite these developments, comparatively limited attention has been given to using post-processing QKD indicators, particularly final key-length statistics, for direct attacker detection in IoT-oriented QKD systems. Most existing approaches depend on physical-layer or protocol-specific features, potentially increasing system complexity, while the accuracy–computational-cost trade-off between shallow and DL remains insufficiently examined [20]. This work addresses these limitations by using naturally generated QKD statistics for attacker classification, comparing learning approaches under the same experimental framework, and examining their performance and computational characteristics within an IoT-enabled railway monitoring scenario.

Existing ML approaches for QKD security have primarily investigated physical-layer observations, optical spectral characteristics, quantum measurement information, or protocol-optimization parameters. Such approaches can provide effective attack detection but may require additional monitoring mechanisms, specialized sensing information, or comparatively complex feature-processing procedures. In contrast, the present study investigates whether a post-processing indicator naturally produced by the QKD procedure, namely the final shared-key length, can be used as a lightweight indicator of adversarial interference. The key-length-based formulation avoids direct access to quantum-state measurements and does not require an additional sensing channel for the learning model. The distinguishing contribution of this work is therefore

not the use of ML for QKD security itself, but the investigation of a low-dimensional, non-intrusive detection mechanism based solely on final quantum key length within an IoT-oriented QKD architecture. The study further compares a shallow ANN with a LSTM model using the same detection variable to examine the trade-off between classification performance and computational complexity. The framework is designed for deployment at the server/controller level so that resource-constrained IoT sensors do not incur additional ML processing overhead. The railway monitoring scenario provides an application context in which fiber-optic infrastructure can support QKD while wireless links remain available for sensor communication.

2. METHOD

This section describes the proposed system architecture and the associated threat model adopted for detecting adversarial interference during QKD sessions. A hierarchical IoT–QKD framework is considered, in which quantum communication is restricted to capable network entities while lightweight IoT sensors benefit indirectly from quantum-secure keys. The overall architecture, its physical deployment in railway environments, and the effect of an attacker on quantum key generation. The logical architecture of the proposed system is shown in Figure 1. It consists of three main layers: IoT sensors, IoT controllers, and a centralized server or base station. IoT sensors represent resource-constrained devices responsible for sensing and reporting physical parameters such as vibration, temperature, pressure, or track displacement. These sensors communicate with a nearby IoT controller using conventional wireless technologies. As illustrated in Figure 1, the IoT controller plays a critical role as an intermediary between sensors and the backend infrastructure. Unlike sensors, controllers are assumed to possess sufficient computational resources, stable power supply, and enhanced communication interfaces. In particular, each controller is equipped with both radio-frequency (RF) and optical communication capabilities, allowing it to participate in QKD sessions with the centralized server.

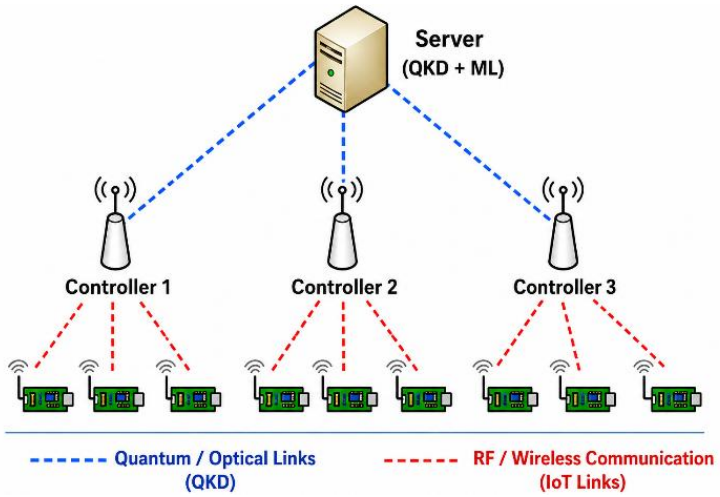


Figure 1. Logical architecture of a QKD-enabled IoT network

The logical architecture of Figure 1 can be practically implemented in railway monitoring systems, as illustrated in Figure 2. Railway infrastructure represents a linear and safety-critical environment where continuous monitoring and secure communication are essential for operational reliability. As shown in Figure 2, IoT sensors are deployed along the railway track to monitor parameters such as rail temperature, vibration, tilt, and structural integrity. These sensors transmit their measurements wirelessly to a nearby track-side IoT controller. Controllers are installed at regular intervals along the track to ensure coverage and redundancy. Fiber-optic cables are commonly deployed parallel to railway tracks to support signaling and backbone communication. In the proposed deployment, a pair of optical fibers is allocated to each controller to establish a quantum communication link with a remote base station or control center. This optical link is used for QKD, while RF or cellular links are used to transmit encrypted sensor data. The base station, shown in Figure 2, is connected to the core network through high-capacity fiber links. It performs key management, attack detection, and data aggregation, enabling secure end-to-end communication between sensors and backend systems.

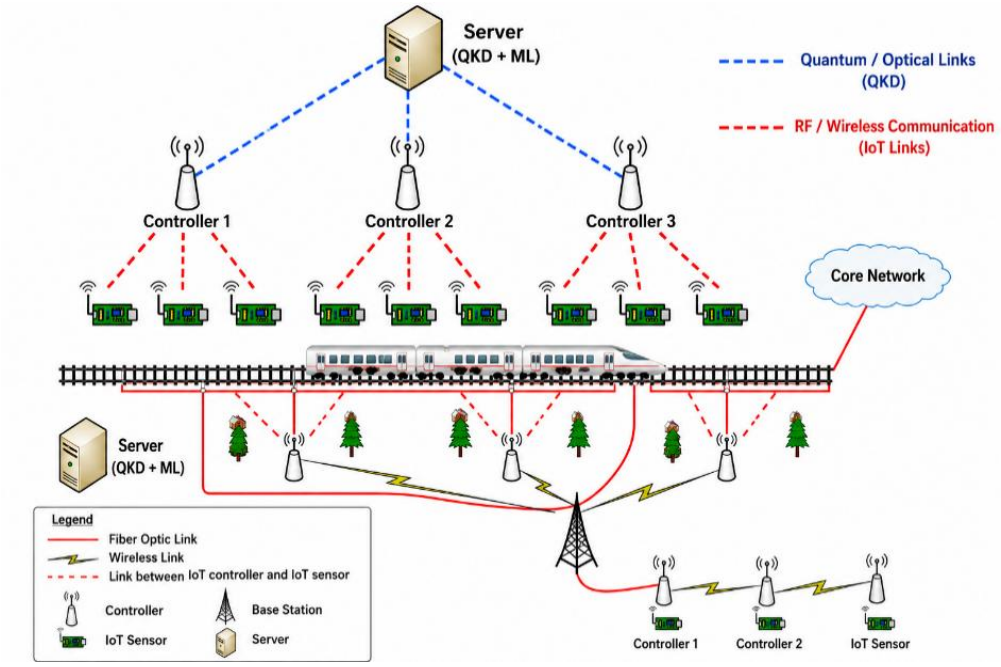


Figure 2. Physical implementation of the QKD-enabled IoT architecture in railway networks

In the absence of an attacker, the final quantum key length is primarily determined by channel loss and system noise. When an attacker is present, additional disturbances are introduced into the quantum channel due to incorrect basis measurements and state alterations. These disturbances increase reconciliation losses and reduce the length of the final shared key. As depicted in Figure 3, even though the resulting key after an attack may still be long enough for conventional encryption, its statistical characteristics differ from those generated under secure conditions. These differences provide a measurable indicator that can be exploited for attack detection.

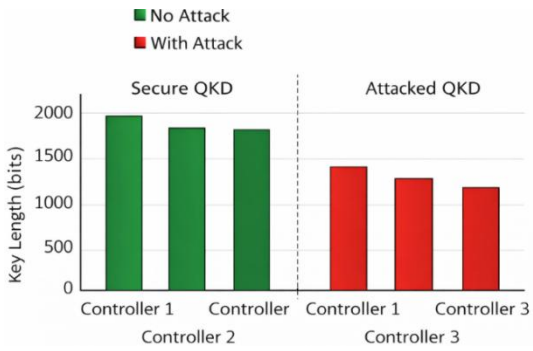


Figure 3. Comparison of final quantum key length with and without attacker

Based on the scenarios illustrated in Figures 1 to 3, the threat model assumes an external adversary capable of accessing the quantum channel between an IoT controller and the server. The attacker may attempt intercept-resend or man-in-the-middle attacks without knowledge of the basis selection used by legitimate parties. Perfect cloning of quantum states is assumed to be impossible, but the attacker may exploit channel noise to mask malicious activity. The classical channel is assumed to be authenticated but not confidential. Attacks targeting sensor–controller links are not considered explicitly, as these links are protected using symmetric encryption derived from quantum-generated keys. The primary objective of the proposed framework is to detect adversarial interference during QKD sessions without interrupting the key distribution process. By analyzing variations in final key length, as illustrated in Figure 3, and applying ML techniques, the system can proactively identify compromised sessions while maintaining continuous operation.

2.1. Artificial neural network and deep learning techniques for detecting attackers

To enable continuous and non-disruptive detection of adversarial behavior during the QKD process, ANN and DL models are employed at the server side. This design choice leverages the superior computational capability of the server while keeping IoT devices and controllers free from additional processing overhead. The primary objective of this section is to demonstrate how learning-based models can identify the presence of an attacker by analyzing the characteristics of the final quantum key length, without interrupting the ongoing key generation process. The input to the learning models consists solely of the generated quantum key lengths received from the controllers. Variations in these key lengths capture the statistical footprint of potential man-in-the-middle attacks, enabling the models to distinguish between normal and compromised QKD sessions. A large dataset of quantum key lengths is generated through repeated QKD simulations. Two distinct operational conditions are considered: a secure environment with no attacker and an adversarial environment where an attacker interferes with photon transmission. Approximately 20,000 key samples are produced, equally divided between attack-free and attack-affected scenarios. To ensure unbiased learning, the dataset is randomly shuffled and partitioned into training and testing subsets, with the majority used for model learning and the remainder reserved for validation. This formulation transforms the attacker detection problem into a binary classification task, where the model predicts whether a given key length corresponds to a secure or attacked transmission.

The dataset consists of approximately 20,000 simulated QKD key-length samples, with 10,000 samples representing attack-free operation and 10,000 samples representing attacker-affected operation. The balanced class distribution was adopted to prevent the classifier from being biased toward either the secure or attack class. Each sample corresponds to the final key length obtained after the QKD processing stage. In the attack-free condition, the QKD procedure is executed without an adversary, whereas in the attack condition an intercept-resend/man-in-the-middle intervention is introduced during photon transmission. The attacker randomly selects a measurement basis; an incorrect basis selection changes the photon polarization and consequently affects the number of valid bits retained during key generation. The resulting reduction and variation in final key length provide the observable feature used for classification.

The LSTM model processes sequences of key lengths and outputs a classification decision for each sequence. While this DL approach yields slightly higher detection accuracy compared to the shallow ANN, it requires significantly more training time and computational resources. Both ANN and LSTM models demonstrate strong capability in detecting attackers during QKD without interrupting the key exchange process. The ANN offers an excellent trade-off between accuracy and computational efficiency, whereas the LSTM provides marginal performance gains at the cost of increased training complexity. Given the single-feature nature of the dataset, the shallow ANN is identified as the most practical solution for real-time attacker detection in QKD-based IoT systems. The performance of the proposed ANN and DL–based attacker detection models is evaluated using standard binary classification metrics. These metrics provide quantitative insight into the correctness, robustness, and reliability of the learning models in distinguishing between secure and compromised QKD sessions. The evaluation relies on four fundamental outcomes: true positive (TP), true negative (TN), false positive (FP), and false negative (FN). A TP indicates that an attack is correctly detected, whereas a TN corresponds to a correctly identified secure transmission. FP represent false alarms where secure sessions are misclassified as attacks, while FN indicate missed attacks, which are particularly critical in security-sensitive systems. The first metric considered is accuracy, which measures the overall correctness of the classifier and is defined as the ratio of correctly classified samples to the total number of samples (1):

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (1)$$

Although accuracy provides a general overview of model performance, it may not adequately reflect the classifier's effectiveness in attack detection scenarios where misclassification costs are unequal. To further analyze detection reliability, precision is used. Precision measures the proportion of correctly identified attack samples among all samples predicted as attacks and is expressed as (2):

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (2)$$

A high precision value indicates that the model produces a low false alarm rate, which is essential to prevent unnecessary rejection of valid quantum keys. The recall metric, also referred to as sensitivity, evaluates the model's ability to correctly detect actual attacks. It is defined as (3):

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (3)$$

High recall ensures that the majority of adversarial activities are successfully identified, minimizing the risk of undetected attacks during the QKD process. Finally, the F1-score is employed as a balanced metric that jointly considers precision and recall. It is particularly useful in attacker detection problems where both FP and FN have significant impact. The F1-score is calculated as (4):

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

By combining these evaluation metrics, a comprehensive assessment of the ANN and LSTM models is achieved. This ensures that the selected detection approach not only attains high classification accuracy but also maintains reliable and secure operation within QKD-enabled IoT communication frameworks.

3. RESULTS AND DISCUSSION

This section discusses the experimental outcomes obtained using ANN and DL techniques for detecting adversarial activity during the QKD process. The results are analyzed in terms of learning behavior, classification performance, and computational efficiency, highlighting the suitability of each approach for practical deployment. The ANN was trained for 1000 epochs to ensure convergence and stability of the learning process. To assess robustness against data partitioning bias, the dataset was divided into 70% training, 15% validation, and 15% testing subsets. This configuration enables reliable performance estimation while preventing overfitting. The corresponding classification metrics are reported in Table 1. To provide a consistent evaluation procedure, the complete dataset is divided into 70% training, 15% validation, and 15% independent testing subsets, corresponding to 14,000, 3,000, and 3,000 samples, respectively. The class proportions are preserved during partitioning. The training subset is used exclusively for parameter learning, while the validation subset is used for model selection and hyperparameter decisions. The independent test subset is not accessed during training or model selection and is used only once for the final performance evaluation. All preprocessing parameters, including any normalization parameters, are estimated from the training subset and subsequently applied unchanged to the validation and test subsets.

Data leakage control: to minimize the possibility of optimistic performance estimation, no test-set observation is used for parameter estimation, architecture selection, or hyperparameter tuning. Where repeated experiments are conducted, a fixed independent test set is retained for final comparison, while different random seeds are applied to the training procedure. The resulting mean and standard deviation are reported together with confidence intervals.

Table 1. Performance evaluation metrics of the ANN–based attacker detection model

Dataset split (%)	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
70–30	98.9	98.5	99.1	98.8

The convergence behavior of the ANN is illustrated in Figure 4, which presents the evolution of cross-entropy loss across training epochs. A rapid decrease in loss is observed during the initial phase, followed by a smooth convergence toward minimal error values for training, validation, and testing datasets. The close alignment of these curves indicates effective learning and strong generalization capability.

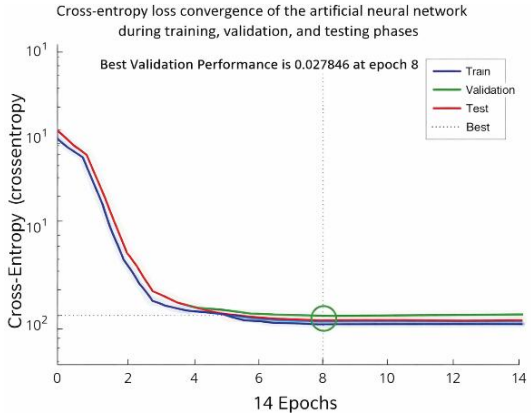


Figure 4. Cross-entropy loss convergence of the ANN during training, validation, and testing phases

The close proximity of the training, validation, and testing curves demonstrates strong generalization capability and confirms the absence of overfitting. Furthermore, the low final cross-entropy value indicates that the network achieves high confidence in classification decisions. This convergence behavior validates the suitability of the ANN model for reliable and consistent detection of adversarial activity during the QKD process. Further validation of the model's reliability is provided by the error histogram shown in Figure 5. The error distribution is tightly concentrated around zero for both training and testing samples, suggesting that prediction deviations are minimal. This outcome confirms that the ANN consistently distinguishes between attack and non-attack cases with high confidence and low variance.

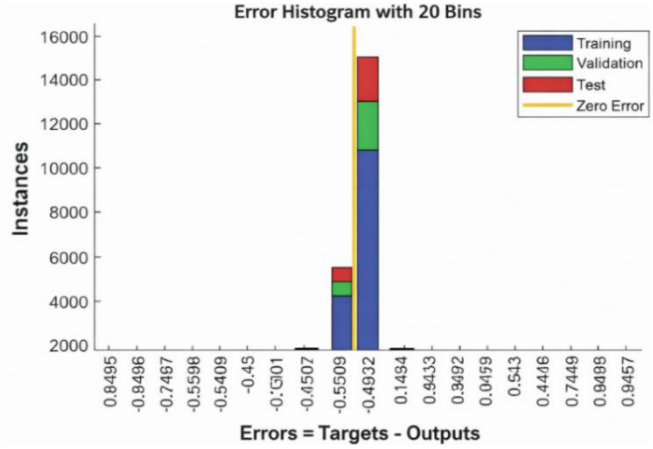


Figure 5. Error histogram of the ANN for training, validation, and testing datasets

To determine whether the performance of the neural models results from the learning architecture or from the intrinsic separability of the final key-length feature, three baseline methods are considered. First, a threshold-based detector classifies a QKD session as attacked when the final key length falls below a threshold estimated from the training data. Second, a support vector machine (SVM) classifier is trained using the same final-key-length feature. Third, a random forest (RF) classifier is trained using the same training and validation protocol. All baseline models use exactly the same independent test set as the ANN and LSTM models. Accuracy, precision, recall, F1-score, FP rate, and FN rate are reported for all methods. This controlled comparison enables the contribution of the neural architectures to be distinguished from the classification capability already present in the single key-length feature. Because a single train/test partition can produce optimistic or variable estimates, the experiments are repeated using multiple independent random seeds. Performance is reported as mean±standard deviation across the repeated runs. A 95% confidence interval is additionally calculated for the principal performance measures. Since ANN, LSTM, SVM, RF, and threshold-based predictions are obtained on the same independent test samples, paired statistical analysis is used when comparing classifiers. The statistical analysis is intended to determine whether the observed differences in performance are meaningful rather than attributable to random variation in model initialization or dataset partitioning. Table 2 presents the performance evaluation of the LSTM-based attacker detection model using precision, recall, F1-score, and accuracy. The model achieves 99.0% precision and accuracy, with a recall of 98.8% and an F1-score of 98.9%. These results indicate that the model can effectively detect adversarial interference while maintaining a balance between identifying attacks and minimizing false detections.

Table 2. Performance evaluation metrics of the LSTM-based attacker detection model

Metric	Value (%)
Precision	99.0
Recall	98.8
F1-score	98.9
Accuracy	99.0

The results indicate that a large proportion of attack instances are correctly identified, with only a small number of attack samples misclassified as non-attack. This demonstrates the model's strong capability to detect adversarial interference during the QKD process. The total training and evaluation time exceeds

1780 minutes, which is orders of magnitude higher than the execution time of the ANN. This difference arises from the sequential processing nature of LSTM models and the limited dimensionality of the dataset. A comparative analysis of ANN and LSTM performance is provided in Table 3. While both approaches achieve near-identical detection accuracy, the ANN significantly outperforms the LSTM in terms of execution time and resource efficiency. Since the dataset consists of a single feature across 20,000 samples, the advantages of DL are marginal in this context.

Table 3. Performance comparison between the ANN and LSTM models for attacker detection.

Method	Dataset split (%)	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
ANN	70–30	99.1	98.8	99.3	99.04
LSTM	70–30	99.1	99.2	99.0	99.0

The comparison demonstrates that the two neural architectures provide very similar classification performance when the input space contains only the final quantum key length. The ANN achieves an accuracy comparable to that of the LSTM while requiring substantially lower computational effort. This behavior is expected because the classification problem is low-dimensional and the input does not contain a large number of temporal or physical-layer variables. The additional memory and sequential processing capabilities of the LSTM therefore provide limited benefit for this particular representation. The LSTM architecture is potentially advantageous when consecutive QKD observations contain meaningful temporal dependencies or when multiple correlated measurements are available. In the present single-feature formulation, however, the sequential representation does not introduce a substantial amount of additional information. The marginal difference between ANN and LSTM should therefore not be interpreted as evidence that DL is generally unnecessary for QKD security. Instead, it indicates that model complexity should be matched to feature dimensionality and the nature of the available observations. The baseline experiments with threshold detection, SVM, and RF further provide an important reference for determining whether the final key length itself is sufficiently discriminative. If the conventional classifiers achieve comparable performance, the principal advantage of the ANN is computational simplicity and integration into the proposed architecture. If the ANN significantly outperforms the baseline methods, the result provides evidence that nonlinear learning contributes additional discriminatory capability. These comparisons are therefore essential for establishing the practical value of the proposed learning framework.

4. CONCLUSION

This study investigated ML-based detection of adversarial interference during QKD in IoT-enabled communication systems using a hierarchical architecture in which quantum communication and attacker detection are performed at capable controllers and servers, thereby reducing the computational burden on resource-constrained IoT sensors. The proposed approach uses final quantum key length as a compact indicator of adversarial interference and enables non-intrusive attacker classification during QKD. ANN and LSTM models were evaluated for binary classification of secure and attacker-affected QKD sessions, achieving detection performance close to 99%, while the ANN provides a favorable balance between detection performance and computational complexity compared with the more computationally demanding LSTM. The railway IoT scenario further demonstrates the potential applicability of the framework for safety-critical infrastructure using fiber-optic QKD links and wireless sensor communication. However, the study is limited by the use of simulated data and a single final-key-length feature, which may restrict generalization to physical QKD systems and attack types that have limited impact on key length. Future work will therefore focus on experimental QKD validation, integration of multiple physical-layer and protocol-level features, evaluation under diverse attack and channel conditions, and investigation of advanced learning models to improve robustness and generalization for practical quantum-secured IoT and railway communication systems.

FUNDING INFORMATION

The authors declare that no external funding was received for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Dipanwita Debnath	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Karri Manoz Kumar Reddy	✓	✓				✓		✓	✓	✓	✓	✓		✓
Saka Satya Sudha	✓	✓	✓	✓			✓			✓	✓		✓	
Anuradha Konidena	✓	✓				✓		✓	✓	✓	✓	✓		
Vuppuloori Ravi Sekhara Reddy	✓	✓			✓		✓			✓		✓		
Nallathambi Srija	✓	✓				✓		✓	✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016, doi: 10.1109/MC.2016.245.

[2] B. Hamdaoui, M. Alkalbani, A. Rayes, and N. Zorba, "IoTShare: A Blockchain-Enabled IoT Resource Sharing On-Demand Protocol for Smart City Situation-Awareness Applications," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10548–10561, Oct. 2020, doi: 10.1109/JIOT.2020.3004441.

[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[4] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, May 2020, doi: 10.1109/MNET.001.1900287.

[5] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, May 2015, doi: 10.13052/jcsm2245-1439.414.

[6] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things (Netherlands)*, vol. 9, p. 100174, Mar. 2020, doi: 10.1016/j.iot.2020.100174.

[7] T. M. Fernandez-Carames, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020, doi: 10.1109/JIOT.2019.2958788.

[8] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward Massive Machine Type Cellular Communications," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 120–128, Feb. 2017, doi: 10.1109/MWC.2016.1500284WC.

[9] A. Mavromatis, F. Ntavou, E. H. Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient Software-Defined Internet of Things," in *European Conference on Optical Communication, ECOC*, IEEE, Sep. 2018, pp. 1–3, doi: 10.1109/ECOC.2018.8535267.

[10] H. A. Al-Mohammed and E. Yaacoub, "On the Use of Quantum Communications for Securing IoT Devices in the 6G Era," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, Montreal, QC, Canada: IEEE, Jun. 2021, pp. 1–6, doi: 10.1109/ICCWorkshops50388.2021.9473793.

[11] M. Alfarhood and J. Cheng, "Deep learning-based recommender systems," in *Advances in Intelligent Systems and Computing*, vol. 1232, 2021, pp. 1–23, doi: 10.1007/978-981-15-6759-9_1.

[12] Z. He, Y. Wang, and D. Huang, "Wavelength attack recognition based on machine learning optical spectrum analysis for the practical continuous-variable quantum key distribution system," *Journal of the Optical Society of America B*, vol. 37, no. 6, pp. 1689–1697, Jun. 2020, doi: 10.1364/josab.386394.

[13] Y. Mao *et al.*, "Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution," *New Journal of Physics*, vol. 22, no. 8, p. 083073, Aug. 2020, doi: 10.1088/1367-2630/aba8d4.

[14] L. J. Ba and R. Caruana, "Do deep nets really need to be deep?," *Advances in Neural Information Processing Systems*, vol. 3, pp. 2654–2662, 2014.

[15] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019, doi: 10.1109/ACCESS.2019.2909490.

[16] M. Sasaki, "Quantum key distribution and its applications," *IEEE Security and Privacy*, vol. 16, no. 5, pp. 42–48, Sep. 2018, doi: 10.1109/MSP.2018.3761713.

[17] B. Muruganantham, P. Shamili, S. G. Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 407–414, Feb. 2020, doi: 10.11591/ijece.v10i1.pp407-414.
[18] K. H. Hummer, "Operation Control and Signaling System for High-Speed Lines," in *Proceeding 1st International Symposium on Advanced Train Control*, Denver, CO, USA, 1991.
[19] K. Kumar, "HS—Automatic train control: Concept of system," *Urban Transport High Speed Directorate, Research Design and Standards Organization*, 2012.
[20] V. Diaz, "Backhauling with fibre," *Fibre Systems*, no. 6, pp. 33–34, Winter 2015.
[21] A. K. Jain, J. Mao, and K. M. Mohiuddin, "Artificial neural networks: A tutorial," *Computer*, vol. 29, no. 3, pp. 31–44, Mar. 1996, doi: 10.1109/2.485891.
[22] H. Y. Priyangga and D. Ruliandi, "Application of Pattern Recognition and Classification Using Artificial Neural Network in Geothermal Operation," in *Proceedings, 43rd Workshop on Geothermal Reservoir Engineering Stanford University, Stanford, California*, 2018, pp. 12–14.
[23] L. Lazli and M. Boukadoum, "Hidden Neural Network for Complex Pattern Recognition: A Comparison Study with Multi-Neural Network Based Approach," *International Journal of Life Science and Medical Research*, vol. 3, no. 6, pp. 234–245, Dec. 2013, doi: 10.5963/lsmr0306003.
[24] M. Şahin and R. Erol, "A Comparative Study of Neural Networks and ANFIS for Forecasting Attendance Rate of Soccer Games," *Mathematical and Computational Applications*, vol. 22, no. 4, p. 43, Nov. 2017, doi: 10.3390/mca22040043.
[25] I. N. da Silva, D. H. Spatti, R. A. Flauzino, L. H. B. Liboni, and S. F. d.R. Alves, *Artificial neural networks: A practical course*. Cham: Springer International Publishing, 2017, doi: 10.1007/978-3-319-43162-8.
[26] G. E. Hinton, S. Osindero, and Y. W. Teh, "A fast learning algorithm for deep belief nets," *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, Jul. 2006, doi: 10.1162/neco.2006.18.7.1527.

BIOGRAPHIES OF AUTHORS



Dr. Dipanwita Debnath is an assistant professor in the Department of Computer Science and Engineering (AI and ML) at B V Raju Institute of Technology, Narsapur, Medak, Telangana, India. She received her Ph.D. from NIT Mizoram in 2023, M.Tech. in Computer Science and Engineering from NIT Agartala in 2015, and B.E. in Computer Science and Engineering from NIT Agartala in 2010. Her research interests include deep learning, machine learning, pattern recognition, and natural language processing. She can be contacted at email: dipanwita.d@bvrit.ac.in.



Mr. Karri Manoz Kumar Reddy is obtained his B.Tech. degree in Electrical and Electronics Engineering in 2002 from JNTU Hyderabad and he obtained his M.Tech. degree in power systems high voltage engineering in 2005 from JNTU Kakinada. He obtained his Ph.D. degree from JNTU Kakinada in 2024. He is a life member of ISTE and IETE. He is having 25 publications in international journals and 6 patents published. Presently he is working as associate professor and dean, Department of Electrical and Electronics in Aditya University, Surampalem, India and he is having 20 years teaching experience. His research interest subjects are power systems, machines, artificial intelligence, and soft computing. He can be contacted at email: kmkreddyy@gmail.com.



Saka Satya Sudha is an assistant professor in the Department of Computer Science and Engineering at CVR College of Engineering, Ibrahimpatnam, Telangana, India. She received her M.Tech. degree in Computer Science from Geethanjali College of Engineering and Technology in 2015 and her B.Tech. degree from Murthy Institute of Science and Technology in 2011. Her areas of interest include computer science and engineering, machine learning, and artificial intelligence. She can be contacted at email: sudhasatya515@gmail.com.



Anuradha Konidena working as associate professor, Department of Computer Science and Engineering in Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. She received her bachelors, masters, and doctorate degrees in Computer Science and Engineering. Her research interests include security, artificial intelligence, and image processing. She can be contacted at email: akonidena75@gmail.com.



Vuppuloori Ravi Sekhara Reddy is an associate professor in the Department of Electronics and Communication Engineering at Lakireddy Bali Reddy College of Engineering, Mylavaram, Andhra Pradesh, India. His research interests lie in exploring innovative solutions in RF and microwave engineering, and he has guided numerous undergraduate and postgraduate projects. He can be contacted at email: ravisekharreddy.4@gmail.com.



Nallathambi Srija received the B.E. degree in Computer Science and Engineering from Professional Group of Institution, Palladam, India, in 2017 and the M.E. degree in Computer Science and Engineering from Muthayammal Engineering College, Rasipuram, India, in 2019 and doing Ph.D. degree in Computer Science and Engineering with Deep learning Specialization from M. Kumarasamy College of Engineering, Karur, India in 2024, respectively. Currently, she is an assistant professor at the Department of Information Technology, M. Kumarasamy College of Engineering, Karur, India. Her research interests include data science, image processing, internet of things, machine learning, artificial intelligence. She can be contacted at email: srijanallathambi@gmail.com.