ISSN-3139-6593 (Online)

Journal of Interdisciplinary Science &Technology

# An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption

**Prof. Shahid R. Siddiqui [1],Devansh Girish Jadhav [1], Karan Dighole [1],**
**Bhavesh Megha [1], Rakshit Sharma [1]**
[1]Department of Computer Engineering, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India
siddiquishahid1402@gmail.com ,devanshj1212@gmail.com, karandighole2004@gmail.com, meghabhavesh27@gmail.com, rakshitsharmark@gmail.com,

***Corresponding author- Prof. Shahid R. Siddiqui***

***DOI**: 10.5281/zenodo.23888913*

**Abstract:** The number Internet of Things (IoT) devices are growing rapidly. Due to this many new IoT cybersecurity challenges are being introduced. The challenges such as limited computational power on the IoT devices leading to them being continuously exposed to changing network threats making IoT Security difficult. Existing security approaches use techniques like deep learning for intrusion detection, reinforcement learning for adaptive response, data integrity mechanisms, and post-quantum cryptography. However, these techniques are often studied separately. But integrating these techniques still faces some challenges such as higher resource consumption, generalization, adaptive response and practical deployment. This paper proposes an AI driven framework that integrates LSTM based anomaly detection, Q-learning based adaptive response, data integrity verification, and post-quantum cryptographic protection. The framework that has been proposed is designed to address some of the challenges such as to detect abnormal behaviour in the network. The framework will also assess the threat level and select the appropriate response and provide additional security to the IoT devices. This framework will be evaluated using datasets such as CICIoT2023 and Edge-IIoTset, with the main focus on computational overhead, performance of detection system, cross-dataset generalisation and adaptive response. This security system approach aims to provide improved resilience and security for IoT environments with consideration of limited resources.

**Keywords:** IoT security, LSTM, anomaly detection, reinforcement learning, Q-learning, data integrity, post-quantum cryptography

## I INTRODUCTION

The Internet of Things has become a large part of the modern computing resulting into large number of devices being connected to network to exchange the data and provide automated services. These kinds of devices are in the areas ranging from a smart watch to smart homes to health care. These devices are also used in the industries making IoT based networks one of the biggest networks to exist. These leads to it being vulnerable to threats at a large scale. As these devices have low computational power, it is challenging to implement strong security mechanisms. The main challenge they face is making the IoT devices more secure [8], [9].

Due to these reasons Intrusion Detection System (IDS) has become an important part of the IoT security. The traditional approaches mainly rely on the predefined rules or known attacks. They work really well if the attack has been predefined in the rules or it's a known attack but if the attack is not defined in the rules then IoT device might get compromised. Due to this, research has been conducted on the machine learning and deep learning being used in IDS to improve its ability to identify complex patterns in the network traffic [2], [3]. The models that are mainly used are Recurrent Neural Network (RNN) and Long Short-term Memory (LSTM) to learn the various patterns from sequential network data [2], [3]. But these models don't fully solve all the challenges as they have some of their own issues as in the dataset dependency, generalization to unseen attacks, computational requirements and mainly practical deployments as they are tested only on the controlled environment [2], [3], [10].

Attack detection is only one part of the IoT security, as the system also needs to respond to detected attacks. Reinforcement Learning provides a possible approach by allowing an agent to learn from the previous patterns and select appropriate response [4], [5]. But even after all this the main issues complexity, scalability, resource consumption and robustness are remaining [4], [5]. On the other hand, the data

© 2026 JIST All Rights Reserved 

integrity mechanisms can help the system identify unauthorized modifications and Post-Quantum Cryptography (PQC) can provide protection against future quantum computing threats [6], [11]. But due to these features the additional complications such as computation, memory, key-size and communication overhead are introduced [6], [11].

The base paper provides a foundation by combining LSTM based anomaly detection, reinforcement learning based responses, data integrity protection, and PQC for protection against attacks enabled by future quantum computers. The issues such as practical deployment, robustness, efficiency and generalization are requiring further investigation [1]. On the basis of this, a framework integrating these four technologies, LSTM based anomaly detection, Q-Learning for appropriate response, data integrity protection and PQC protection is introduced [1]. The evaluation of the framework will be done using IoT datasets focusing on detection performance, cross dataset generalization, adaptive responses and the overhead introduced by the security mechanism.

## II. PROBLEM STATEMENT

IoT has a very large network of devices and these devices have different capabilities and limited computational resources, making the implementation of the effective security difficult [8], [9], [10]. Traditional Intrusion Detection System (IDSs) have a problem they mainly depend on predefined rules and known attacks and they work really well on those attacks but when it comes to new or unknown threats they fail to detect them. Machine learning and deep learning can improve attack detection but they still face the issues such as dataset dependency, computational power, generalization and practical deployment [2], [3], [10]. Attack detection also requires its appropriate response based on the severity of the threat. Reinforcement Learning (RL) provides the appropriate response but it has a bit of drawback as it resource requirements and complexity must be considered [6], [7], [11]. Data integrity and protection through PQC introduce more complexities like computational and communication overhead. Therefore, an integrated approach is needed to combine detection, adaptive response, integrity protection, and PQC security while considering IoT resource limitations.

## III. BACKGROUND AND DEFINITION

### A. IoT Cybersecurity

The IoT consists of connected devices that communicate and exchange data through networks. These IoT devices are used in various places ranging from smart watches to smart homes and healthcare and other applications. One drawback that these IoT devices have is that they have low computational power leading to them having limited security mechanisms implemented in them [8], [9].

### B. LSTM-Based Intrusion Detection

An Intrusion detection system (IDS) is used to detect malicious or suspicious activity in network traffic. The traditional approaches mainly depend predefined rules and known attacks, they work well if the attack is defined on these rules but if an attack that is not defined in the rules or some unknown attack occurs the system fails miserably. Machine learning and deep learning are methods that can be used to address these issue as they can be used to identify more complex patterns in the network traffic [2], [3]. Long Short Term Memory (LSTM) can be used to retain the information from previous inputs and also feeds on sequential data [2], [3].

### C. Reinforcement Learning And Q-learning

Reinforcement Learning (RL) is a machine learning approach which is based on basis of reward system. An agent interacts with the environment and learns actions based on the state of the environment and reward is provided to the agent [4]. RL is a mechanism that can be used to select the responses after detecting a threat [4], [5]. Q-learning is a RL algorithm that is based on the fact that it learns the expected value of different actions for different states making it very good candidate for selection of appropriate response after a threat is detected [4], [5].

### D. Data Integrity and Post-Quantum Cryptography

Data integrity is an important part of IoT network as the IoT devices share information continuously through the network. This data can be modified and or tampered with. Various integrity mechanism can be used to verify if the data has been tampered or not [7], [9]. Post-Quantum Cryptography (PQC) refers to cryptographic technique used to remain secure from the quantum computers [6], [11]. Traditional protection techniques are not good protection against attacks enabled by future quantum computers to tackle this PQC can be used. PQC's drawbacks include of larger keys, cipher texts and computational requirements, which leads to additional overhead [6], [11].

## IV. RELATED WORK

### A. Deep Learning for IoT Intrusion Detection

Several studies have implemented deep learning and machine learning in IDS due to its effectiveness. Models such as RNN, CNN and LSTM have been used through various studies to identify the threats and malicious activity in network traffic [2], [3], [10]. Best thing about these models is that they adopt to networks and traditional rule based detection don't as they are rule based approaches. But that doesn't mean that they don't have any problems, issues such as dataset dependency, detection of unseen attacks, computational requirements and practical deployment remain challenges.

© 2026 JIST All Rights Reserved 

### B. Reinforcement Learning for Adaptive security

Researchers have also explored Reinforcement Learning (RL) and Deep Reinforcement learning (DRL) for increasing the adaptability of IoT security [4], [5]. RL allows the agent to learn specific actions for specific task through the state of the environment and rewards received [4]. This helps system select appropriate response to different levels of threat [4]. The challenges such as training complexity, scalability, resource management, and robustness still remain [4], [5].

### C. Data Integrity and Adaptive Security

Data integrity mechanism helps in detecting if the IoT data has being modified by an unauthorised personal [7], [9]. PQC has also been checked for been investigated for protect communication against future quantum computers. Due to the challenges like computational power, memory, key-size and communication overhead are also introduced [6], [11].

### D. Integrated IoT security Frameworks

The base paper combines LSTM-based anomaly detection, reinforcement learning, data integrity protection, and PQC into an integrated IoT security framework [1]. It provides a foundation for combining different security mechanisms, but challenges related to practical deployment, resource efficiency, generalization, robustness, and overhead remain [1], [5], [11]. These limitations provide the basis for further investigation in this study.

## V. RESEARCH GAP

Existing research has investigated different approaches for improving IoT security, including deep learning-based intrusion detection, reinforcement learning for adaptive response, data integrity mechanisms, and post-quantum cryptography [2]-[7], [9]-[11]. Some studies have also explored integrating multiple security mechanisms into a single framework [1]. However, challenges related to resource efficiency, generalization to different attack conditions, robustness, practical deployment, and the overhead introduced by multiple security mechanisms remain [2], [3], [5], [10], [11]. The base paper provides an integrated foundation using LSTM, reinforcement learning, data integrity, and PQC, but these areas still require further investigation [1]. Therefore, this study focuses on evaluating an integrated framework with emphasis on detection performance, cross-dataset generalization, adaptive response, and the computational and communication overhead of the security mechanisms.

## VI. PROPOSED FRAMEWORK

The proposed framework integrates four main security components: LSTM-based anomaly detection, Q-learning based adaptive response, data integrity verification, and post-quantum cryptographic protection [1]. IoT network traffic will be processed and provided to the LSTM model for identification of abnormal behavior. The Threat that has been detected gives the information which can be used by Q-learning agent for the selection of the appropriate response based on the threat state. The data integrity mechanisms will be used to identify the unauthorized modifications to IoT data and PQC will provide additional protection for sensitive communication and data transfer. The framework will have the ability to connect these components to the backend system using Spring Boot and MySQL for processing and storing all security-related information. A real-time dashboard built using React will be used to display security-related information, including detected threats and selected responses. Docker will be used to containerize the major components of the framework to simplify deployment and management.

## VII. METHODOLOGY

The framework methodology will begin with collection and preprocessing IoT network traffic from CICIoT2023 and Edge-IIoTset will be used for cross-dataset evaluation. The data that will be collected will be normalized, cleaned and prepared as sequential data for LSTM model. The LSTM model will be trained for the identification of normal and abnormal patterns present in the network traffic providing information about the threats that will be detected. This information from the threats will be used by Q-learning agent as part of the threat state for the learning and selection of an appropriate security response. Data integrity verification will be applied for the identification of unauthorised modifications in the data. PQC will be used for providing additional protection for communication and data. The security components will be integrated using Spring Boot and MySQL will be used for storing security related data and processing. A React Dashboard will be used for displaying threats and response to that particular threat. This framework will be evaluated by using detection metrics, cross-dataset performance, response effectiveness and computational and communication overhead introduced by security mechanism.

## VIII. EVALUATION PLAN

The evaluation of this proposed framework will be done using different performance measures for each security component. The LSTM based detection model will be evaluated using false positives rate, F1-score, accuracy and precision. Cross-dataset testing will be performed to study the generalization of the detection model across different IoT network traffic conditions. The evaluation of the Q-learning component will be based on the effectiveness and the response time of the selected security actions rather than traditional response methods. The data integrity mechanism will be evaluated by seeing its ability to detect the modifications in data and the overhead introduced during verification. PQC evaluation will be based on cryptographic operation time, key and ciphertext size, and

© 2026 JIST All Rights Reserved 

additional computational and communication overhead. The overall framework will also be evaluated for resource usage and system performance.

## IX. EXPECTED OUTCOMES

The expected outcome from LSTM model is to detect normal and abnormal IoT network traffic. Cross-dataset testing is expected to show how well the detection model generalizes to different IoT traffic conditions. Q-learning's expected outcome should be selection of appropriate response based on detect threat state. The outcome expected from Data integrity verification is to detect of unauthorised modifications in the data. PQC will provide additional protection against attacks enabled by future quantum computers for communication and data. This evaluation should also provide information about overhead that is introduced by these security mechanisms. Overall this framework is expected to provide more integrated approach for IoT security. This approach will provide detailed information about cyber-attacks with the integration of these technologies.

## X. PROJECT FOCUS AND FUTURE DIRECTIONS

The main focus of this project will be on the implementation and evaluation of proposed integrated IoT cybersecurity framework. The project will focus in detection of abnormal IoT network traffic using LSTM, selection of appropriate response using Q-learning, detections of unauthorized modifications through data integrity verification and PQC for adding protection of communication and data, to this framework. This framework will also focus on studying cross-dataset generalization and the computational and communication overhead introduced by the security mechanisms.

The direction this project will take in future will be on improvement of the framework by implementation of adaptive anomaly thresholds, explainable AI for the better understanding of LSTM detection results, and more advanced Q-learning response strategies. The framework can also be extended for large-scale IoT environments and can be tested under more realistic conditions to study its scalability, robustness and resource efficiency.

## XI. CONCLUSION

IoT security is difficult to navigate due to having large number of devices and those devices having resource limitations. The proposed framework integrates four technologies: LSTM-based anomaly detection, Q-learning-based adaptive response, data integrity verification and PQC. This frame is designed to detect abnormal behaviour in the IoT network traffic, select appropriate response, identify unwanted modifications in the data and provide additional protection for communication and data. The evaluation of the framework will be done using datasets CICIoT2023 and Edge-IIoTset with focus on detection performance, cross-dataset generalization, response effectiveness, and overhead that is being introduced by these mechanisms.

## XII REFERENCE

[1] M. M. Saeed, "An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption," IEEE Access, vol. 13, pp. 104027–104036, 2025, doi: 10.1109/ACCESS.2025.3576506.

[2] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. U. R. Khan, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," IEEE Access, vol. 12, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.

[3] Alyazia Aldhaheri et al., "Deep learning for cyber threat detection in IoT networks: A review," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 110–128, 2024.

[4] Aashma Uprety and Danda B. Rawat, "Reinforcement Learning for IoT Security: A Comprehensive Survey," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8693–8706, 2021.

[5] Q. A. Al-Haija and S. Al Tamimi, "A State-of-the-Art Survey of Adversarial Reinforcement Learning for IoT Intrusion Detection," Computers, Materials & Continua, vol. 87, no. 1, pp. 1–10, 2026, doi: 10.32604/cmc.2025.073540.

[6] M. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," IoT, vol. 2, no. 1, pp. 71–91, 2021.

[7] J. Abosata et al., "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," Sensors, vol. 21, no. 11, p. 3654, 2021.

[8] S. Sadhu et al., "Internet of Things: Security and Solutions Survey," Sensors, vol. 22, no. 19, p. 7433, 2022.

[9] G. Dritsas and M. Trigka, "A Survey on Cybersecurity in IoT," Future Internet, vol. 17, no. 1, p. 30, 2025.

[10] Komal and X. Li, "Intrusion Detection in the Internet of Things: A Comprehensive Review of Techniques, Architectures, Datasets, and Emerging Trends," Sensors, vol. 26, no. 11, p. 3405, 2026.

[11] L. Liu, G. Ramachandran, and M. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," arXiv preprint arXiv:2401.17538, 2024.

© 2026 JIST All Rights Reserved 