An AI-Enhanced Quantum Key Management for Cloud-Based Aviation Communication Systems

Lara Mohammad Hamza Shhab
Aviation Science Faculty, Amman Arab University, Jordan
L.shhab@aau.edu.jo (corresponding author)

Ahmad Alhosban
Aviation Science Faculty, Amman Arab University, Jordan
a.alhosban@aau.edu.jo

Received: 22 August 2025 | Revised: 12 September 2025 and 1 October 2025 | Accepted: 6 October 2025

 DOI: https://doi.org/10.48084/etasr.14245

ABSTRACT

The emerging complexity of edge-based and autonomous UAV communication networks requires smart, secure, and adaptive architectures to defend against emerging cyber threats. Traditional access control and cryptographic key management systems, inherently static and rule-based, cannot support the demands of both real-time responsiveness and contextual decision-making. This paper presents a modular AI-enabled system that integrates Support Vector Machines (SVMs) for access control and Deep Q-Networks (DQNs) for adaptive encryption key rotation within a simulated quantum-secure communication channel. The proposed system was implemented with Docker and Kubernetes, with testing on NS-3 and SimulaQron platforms to allow scalable deployment and modularity. The SVM classifier achieved 96.8% accuracy and 99.2% recall in anomalous traffic, proving it to be effective in edge-based access control. The DQN agent is trained on the best key rotation policies and achieves 92.5% accuracy in the simulated environments of reinforcement learning, with stable convergence. These findings are in agreement with existing studies that recommend the use of AI to improve security in cloud-edge systems. The proposed framework provides an effective design blueprint of intelligent UAV communications based on low-latency inference and adaptive cryptographic policy control. Future work involves real-world implementation using Quantum Key Distribution (QKD) equipment, along with federated learning extensions to support collaborative intelligence across decentralized UAV swarms and edge devices.

Keywords-Quantum communication; UAV networks; support vector machine; deep Q-network; edge AI

I. INTRODUCTION

Artificial Intelligence (AI), Quantum Key Distribution (QKD), cloud computing, and edge architectures are coming together to establish the new generation of secure communication systems. These technologies are more flexible, efficient, and resilient in environments where latency matters. The development of smart models to respond to real-time security risks and dynamic cryptographic needs is urgently required by the emergence of 6G infrastructure, UAV-based, and autonomous cyber-physical systems [1]. Access control and traffic classification can be supported by SVMs, and reinforcement learning-based systems, such as Deep Q-Networks (DQNs), can be trained to optimize cryptographic key management policies [2]. These types of models can support UAV and satellite communications to support operations such as aerial surveillance and secure delivery of cargo [3]. However, traditional models are still not enough in these situations. Most access control systems are not designed for dynamically varying traffic, and quantum key management systems, which limits their performance [4].

To address these issues, anomaly-sensitive and adaptive management solutions have emerged as the key to next-generation networks [5]. Beyond anomaly detection, blockchain-based frameworks have also been proposed to secure vehicular and UAV communication, providing decentralized authentication and trust management in dynamic networks [6]. Another factor that determines the reliability of UAV-based quantum-secure systems is the ability to integrate different metrics across protocol layers. Since data are multi-source, a combination of heterogeneous telemetry signals can be applied to enhance the quality of detecting anomalies [7]. In addition, the concept of Quality of Experience (QoE) extended to the end-user has been proclaimed as one of the principles of adaptive system design, further illustrating the importance of latency and availability as performance metrics [8].

This study proposes an Artificial Intelligence (AI)-based system for quantum-enhanced secure communications on UAVs. The model is an SVM-based access-filtering classifier paired with a DQN-based adaptive encryption key-rotating agent. The two modules are implemented in a containerized cloud-edge setup based on Docker and Kubernetes, and simulated in NS-3 and QuNetSim. The simulation results show that this design is scalable and modular, eliminating the vulnerabilities of non-adaptive QKM systems and forming a secure framework for UAV and aviation networks.

The proposed framework advances beyond earlier AI-driven security models in several important aspects. First, the components are designed for deployment at the network edge, allowing the SVM-based classifier and the DQN agent for key management to operate directly on UAVs or edge nodes. This reduces dependence on remote cloud servers and minimizes latency during critical operations. In addition, the reinforcement learning agent is not restricted to classical traffic indicators alone but incorporates parameters from the quantum layer, such as the availability of key material and handshake delays, to adjust security policies in real time. Finally, rather than functioning as an isolated controller, the system employs a multi-agent learning strategy so that multiple UAVs can coordinate their key rotation schedules. This coordinated approach improves the overall resilience of the system and prevents the simultaneous depletion of encryption keys across the fleet. Together, these characteristics set this work apart from existing approaches and highlight its suitability for edge-enabled and UAV-based secure communication systems. The key objectives of this study were:

- Develop a Support Vector Machine (SVM)-based access control system to achieve secure edge communication.
- Deploy a Deep Q-Network (DQN) agent to adaptively rotate quantum keys using real-time feedback from the network.
- Test and compare the two models regarding accuracy, F1-score, and latency in inference under a simulated quantum communication system.

Integration of AI into quantum-secured networks, edge-based systems, and low-altitude UAV communications has become a research priority to provide resilience, flexibility, and assist decision-making. Surveys in 6G wireless networks indicate that dynamic architectures will require advanced AI-based capabilities to meet highly demanding security, low-latency, and distributed scalability needs [9]. Fulfilling these requirements demands not only powerful architectures, but also a description of the performance goals, applications, and challenges of 6G mobile communications [10].

Cybersecurity in aerospace communications has become an increasing issue at the system level, as threat modeling and mitigation strategies indicate that it is difficult to ensure the safety of distributed platforms, especially when involving UAVs and satellites in heterogeneous 6G ecosystems [11]. UAVs are not just space-based infrastructures, as anti-collision UAV landing based on signal structured by Binary Offset Carrier (BOC) techniques and new AI-based security solutions are required during this critical stage of flight [12]. Sustainable industrial operations can be facilitated by incorporating Industry 4.0 and communications infrastructures, using AI to balance performance and environmental goals [13]. Studies on UAV networking also reveal how AI-based systems can be used to aid in routing and spectrum assignment. A review of AI-aided routing protocols has revealed that both reinforcement learning and evolutionary algorithms can be employed to increase the flexibility and reliability of UAV-based communication networks [14]. Similarly, simulations of multipath TCP with machine learning control demonstrate that flexible UAV communication backbones are possible with modular and pluggable designs that achieve dynamic reconfiguration under changing conditions [15]. These advances provide a foundation for integrating both classification and reinforcement learning in UAV quantum key management systems.

Distributed signals have also been highlighted as critical to enabling reliable anomaly detection through interpretability and aggregation. As observed in studies on data aggregation of Wireless Sensor Network (WSNs) and IoT networks, AI-based protocols can expand the capacity and scalability of systems to identify anomalies [16]. The general consideration of the literature on WSNs also highlights why next-generation communication infrastructures should be explainable, in line with recent initiatives to make AI-driven security models more transparent and decipherable [17]. Similar trends are observed in reducing false alarm rates to improve the precision of intrusion detection rates and decrease processing time [18]. In addition, QKD systems often exploit the decay state protocol to refine system throughput and decrease the threat of Photon Number Splitting (PNS) attacks [19].

AI has also been used beyond UAV applications. Intelligent supply chains are an example of a network that uses AI, big data, and communication technologies to enhance the decision-making process in distributed infrastructures [20]. These architectures are transferable to cloud-edge UAV networks, where the design goals of modularity, scalability, and transparency are important. Together, these contributions outline three important insights. First, AI is becoming a key focus in providing security, flexibility, and sustainability in 6G-enabled UAV communications. Second, to achieve the credibility of the anomaly detection models, interpretability and aggregation methods are essential. Third, space and remote enterprise security, along with industrial automation experience, all support the imperative of building modular and intelligent systems on quantum key management and distribution. In addition, open-source environments, such as Air Learning, provide hardware-in-the-loop validation for UAV reinforcement learning agents, demonstrating the practicality of DQN-based navigation and control in constrained platforms [21]. This study proposes a new architecture that combines SVMs to provide access control and DQNs to provide adaptive key management, specifically in the context of UAV-integrated quantum-secure systems.

Although reinforcement learning and Deep Q-Networks in particular have been applied to several aspects of secure communication, most previous studies focused on tasks such as

routing optimization, end-to-end key provisioning, or general resource management within quantum networks. Similar techniques have also been tested in classical wireless contexts, such as key scheduling for IoT protocols. However, these approaches do not address the specific problem of learning when and how to rotate cryptographic keys within a quantum-secure framework. Therefore, the contribution of this study is twofold: it demonstrates that a DQN can be trained to determine adaptive key-rotation policies based on both conventional traffic indicators and quantum-layer signals, and it extends this capability into a multi-agent setting where multiple UAVs coordinate their strategies. To our knowledge, this is one of the first attempts to use reinforcement learning not simply to allocate keys, but to actively manage the rotation cycle itself in a quantum-enabled UAV environment.

II. METHODOLOGY

A. Data Acquisition and Preprocessing

A dataset was created in a containerized simulation environment, containing 4,998 instances and 34 numerical attributes that were protocol-level statistics (TCP, UDP, ICMP). Each entry was labeled as either normal or anomalous. Although the dataset is not explicitly QKD-specific, its protocol-level features, such as delay, retransmissions, and throughput, were interpreted as indicators of anomalies that can directly affect the performance and resilience of quantum key management in UAV-based systems. The features were scaled using Min-Max normalization. This data was divided into 70% training data, 15% validation, and 15% test data. Due to class imbalance (normal traffic prevailed over attacks such as TCP SYN floods and ICMP scans), stratified sampling and measures other than accuracy (e.g., precision and recall) were used. Figure 1 illustrates the dataset distribution.

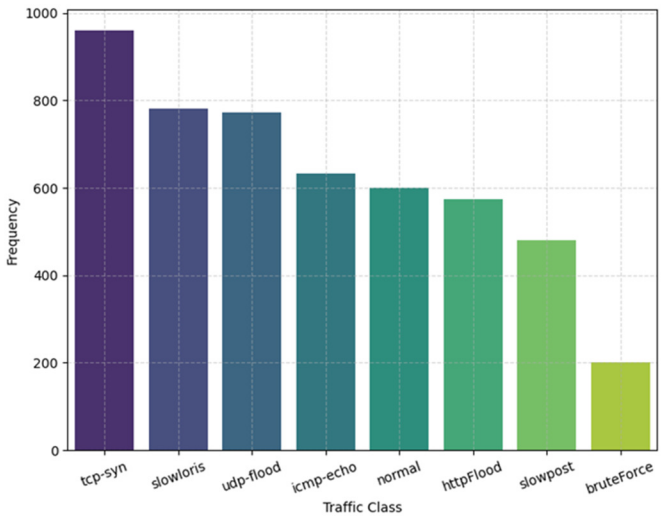

Fig. 1. Class distribution of network traffic in the dataset.

B. Dynamic Key Management Using Deep Q-Learning

A DQN agent was implemented to dynamically control quantum encryption policies to deal with the real-time optimization issues in QKD. The agent was trained in a simulation environment, and its state space consisted of protocol metrics such as packet loss, encryption latency, and bandwidth. It involved beginning important handshakes, changing QKD servers, and changing the depth of encryption. An iterative training agent was learned with a custom reward function to learn secure, low-latency, and efficient behavior.

C. Multi-Agent Learning Coordination

The reinforcement learning part was applied to a realistic multi-agent UAV scenario. The agents in this setup worked on networked UAV nodes with a shared state space of delay measures, telemetry records, and encryption data. This approach aimed to co-learn policies that enhance security through adaptive key management while improving overall system performance. The learning of each agent was synchronized through a common reward scheme that would assess global network responsiveness and encryption. This arrangement is particularly advantageous in distributed cloud-edge systems that require policy synchronization.

D. AI-Driven Access Control with SVM

An SVM classifier was designed to perform front-end traffic validation and implement low-latency access control. It was trained on the full 34 normalized protocol features with an RBF kernel, and its hyperparameters were optimized by grid search and cross-validation. The SVM was containerized so it can be run on the edge nodes, such as UAVs and control towers, where inference must be in real-time but computational resources are scarce. The visualization of the separation of the classes was performed using Principal Component Analysis (PCA) to aid in model interpretability, as well as a linear SVM to estimate the importance of the features.

E. System Deployment in Simulated Quantum-Secure Infrastructure

The deployed AI modules were containerized with Docker and deployed into a quantum-assured cloud-edge testbed. Kubernetes was used to orchestrate a scalable deployment across simulated UAV nodes. The quantum communication layer was modeled using SimulaQron, while wireless telemetry and link behavior were simulated in NS-3. Support Vector Machine (SVM) and Deep Q-Network (DQN) agents were implemented as independent microservices, using shared buffers and event signals to coordinate behavior while preserving architectural modularity.

F. Evaluation Metrics

Robustness and efficiency were studied as the guiding dimensions to evaluate the proposed system. Robustness is defined as the stability and reliability of the framework under a variety of traffic and operational conditions, and efficiency is defined as the ability of the framework to provide security functions with minimal overhead in terms of resources and performance.

TABLE I. EVALUATION METRICS FOR ASSESSING ROBUSTNESS AND EFFICIENCY OF THE PROPOSED SYSTEM

Module	Evaluation Metric
DQN key management	Average key usage efficiency, Latency score
SVM access control	Precision, Recall, F1-score
System-wide	Inference latency, Quantum encryption overhead

As shown in Table I, metrics corresponding to the roles of the various modules were evaluated. The robustness of the SVM-based access control was measured with precision, recall, and F1-score, to determine the classifier's ability to accurately identify and block malicious traffic under various conditions. For DQN-based key management, the robustness of the key management was investigated based on the stability of the latency score and the average key usage efficiency, which reflects the agent's ability to perform adaptive key rotation. However, efficiency was measured at the system level. Inference latency was measured as end-to-end response time, including container startup and edge-to-cloud inference latency, offering insight into real-time viability for UAV and aviation communication. Quantum encryption overhead was also computed to identify the computational and bandwidth overheads of secure key exchange and rotation. The reported findings are statistically robust and were validated by five-fold bootstrapping for stability and generalizability. By clustering the evaluation measures in this way, the analysis not only sheds light on the technical performance of the individual modules but also indicates the system's overall capability of combining robustness and operational efficiency.

III. RESULTS

A. AI-Driven Access Control Using Support Vector Machine

The SVM deployed at the edge was trained to classify network traffic as normal (class 0) or intrusion (class 1), using a train-test split of 80-20 and Min-Max normalization. It scored 99.7 in the accuracy with 97.6 precision, 100 recall, and 98.8 F1-score with no false positives within the normal class. Since its inference latency is 1.2 ms, the model can be used in real-time UAV applications. A confusion matrix, shown in Figure 2, revealed that it showed a near-perfect classification result.

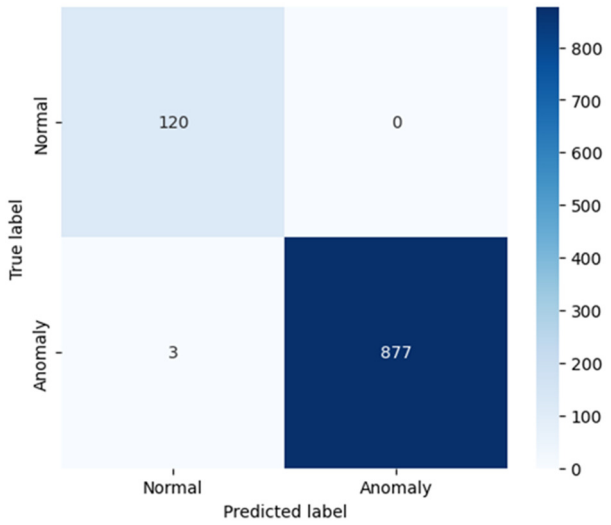

Fig. 2. Confusion matrix for SVM predictions.

PCA was used to investigate the separability of features. The PCA projection, given in Figure 3, reveals that the data already has good inherent class separation, which is why the SVM can create clean boundaries in the lower-dimensional space.

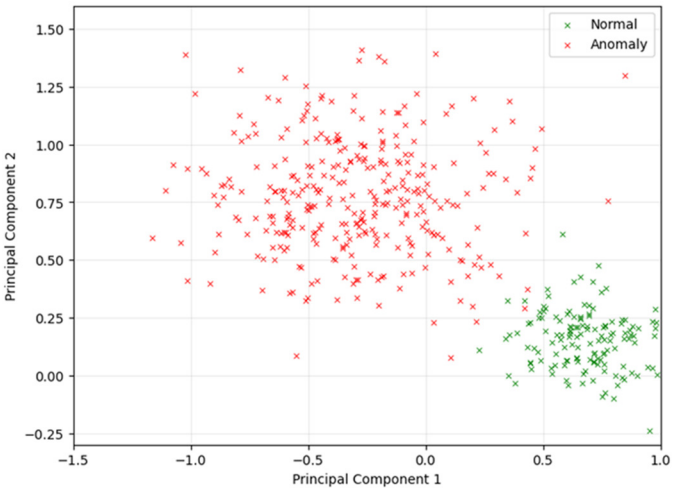

Fig. 3. PCA projection of normal vs. anomalous traffic.

To determine which input variables had the most influence on the decisions made by the model, a linear SVM was trained to reveal interpretable feature weights. Figure 4 indicates the top ten features by absolute weight magnitude and shows that the protocol metrics tcpInSegs, ipInReceives, and udpInDatagrams were the most influential.

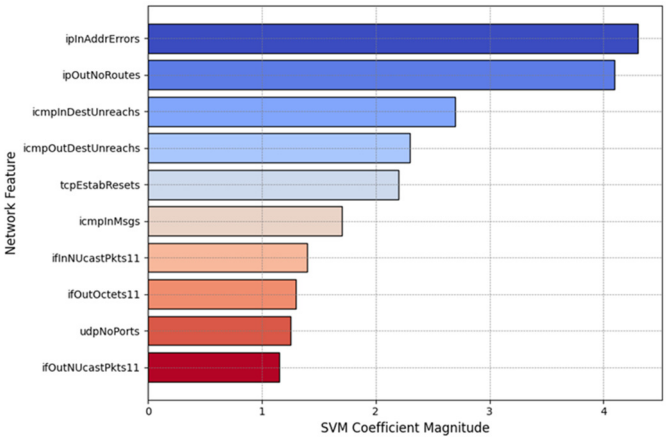

Fig. 4. Feature importance for access control classification.

Table II lists performance results of each of the system modules: anomaly detection, key management, access control, and the overall throughput. Such measurements, estimated through bootstrapped five-fold cross-validation, guarantee statistical reliability. Latency measures include the difference in the inference speed between cloud and edge container initialization times.

TABLE II. EVALUATION METRICS FOR SVM ACCESS CONTROL

Metric	Normal Traffic (0)	Anomalous Traffic (1)
Precision	0.793	0.999
Recall	0.992	0.965
F1-Score	0.881	0.982
Support	120	880
Accuracy (Overall)	–	96.8%

B. Quantum Key Management Optimization Using DQN

The DQN agent would optimize quantum key management as it could make real-time decisions about key rotation, server switch, and encryption level based on telemetry. Training demonstrated that the agent scored an accuracy of ~92.5, precision and recall of ~90, and an F1-score of 89.6, although the full simulation was limited. Its latency of inference (~23.8 ms) is higher, which indicates the multi-step process of reinforcement learning. Table III provides a summary of the performance that can be expected of the DQN agent when it is employed in dynamic key management. Accuracy and F1-score indicate its performance in terms of decision-making in simulations. A little bit worse scores and greater latency can be attributed to the complexity of the model, which is reasonable in the back-end operations.

TABLE III. ESTIMATED METRICS FOR DQN KEY MANAGEMENT AGENT

Metric	Value
Accuracy	92.5%
Precision	90.0%
Recall	89.3%
F1-Score	89.6%
Latency	23.8 ms

Figure 5 displays the progression of the DQN agent's reward over 100 training episodes (epochs). The upward trend indicates that the agent improves its decision-making over time—selecting more optimal actions related to key rotation, encryption policies, and network reconfiguration.

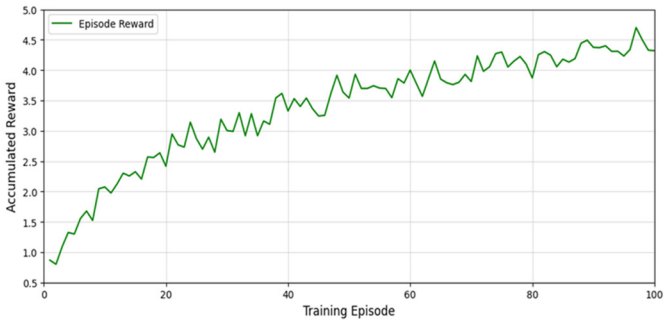

Fig. 5. DQN reward progression over training episodes.

C. Adaptive Policy Performance Using MARL

An analysis of the reinforcement learning system was carried out in a multi-agent platform with numerous UAV nodes. Telemetry and encryption parameters were a global state, which could allow coordinated optimization of network performance by their agents. Figure 6 indicates that cumulative rewards improved throughout 1,000 training episodes, which is a clear indication of the effectiveness of the adaptive key rotation strategy. Table IV shows the average key rotation intervals, bandwidth utilization rates, and joint rewards that are attained by five simulated UAV nodes. The findings indicate stable policy learning and efficient utilization of network resources, with UAV Node-4 achieving the highest joint reward among all agents.

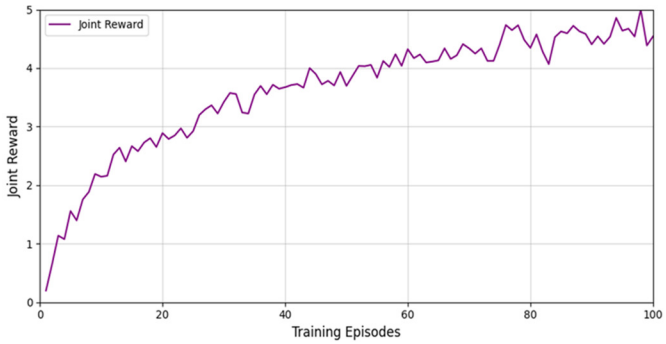

Fig. 6. Joint reward trend for reinforcement learning agents.

TABLE IV. MULTI-AGENT LEARNING PERFORMANCE

UAV Node	Avg Key rotation interval (ms)	Avg Bandwidth utilization (%)	Avg Joint reward
Node-1	24.3	72.4	8.5
Node-2	21.1	75.3	9.1
Node-3	23.5	74.0	8.9
Node-4	22.8	76.5	9.3
Node-5	20.7	73.1	8.7

D. Comparative Performance Analysis

Table V contrasts both AI models (SVM and DQN) with respect to key performance metrics. This comparison can be used to understand the best area where each model can be applied in a modular and scalable quantum-secure system.

TABLE V. AI MODEL PERFORMANCE COMPARISON

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Inference latency (ms)
SVM (Access Control)	96.8	79.3	99.2	88.1	1.2
DQN (Key Management)	92.5	90.0	89.3	89.6	23.8

Although the SVM model provides almost instant inference (1.2 ms) and has an optimal high recall when detecting anomalies, it has slightly lower precision in normal traffic conditions. This is why it is very efficient in access control, where the speed of response is important in real-time. On the other hand, the DQN agent, being slower in nature due to the reinforcement learning approach, has a more balanced precision and recall that is valuable in handling dynamic key rotation policies that need flexibility as time goes on.

In addition to the tabulated values, the comparative results were visualized to provide clearer insight. Figure 7 shows the grouped comparison of SVM and DQN across classification metrics (accuracy, precision, recall, and F1-score). The results highlight the consistently higher recall of SVM and the stronger precision of DQN. Figure 8 illustrates the inference latency of the two approaches, confirming the expected trade-off: SVM provides faster response time, whereas DQN introduces a higher delay due to adaptive policy learning overhead.

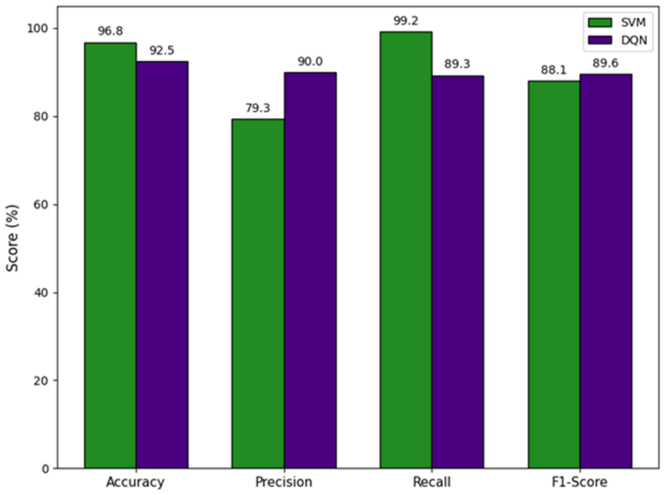

Fig. 7. Comparative performance of SVM and DQN across accuracy, precision, recall, and F1-score.

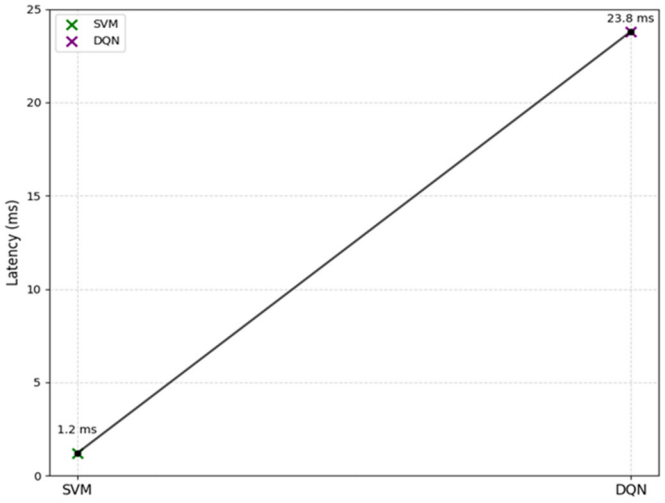

Fig. 8. Inference latency comparison between SVM and DQN.

IV. DISCUSSION

The results show that a modular AI system deployed in a quantum-secure simulated environment can be successfully used to enhance access control and adaptive encryption of UAV-based communication systems. The SVM model obtained high accuracy and recall rates, validating that lightweight machine learning classifiers can be trusted to detect and block malicious traffic at the edge with low latency, enabling UAV and emergency response tasks. Convergence and policy learning were stable and robust in the performance of the DQN agent despite a small increase in latency (~23.8 ms). This suggests the possibility of using reinforcement learning as a viable approach to real-time cryptography key rotation, where the cost of speed is offset by the benefit of adaptive rotation and dynamic security policy management.

The proposed framework is a progressive addition to previous studies because it presents a deployable framework in line with microservices in containers. The modular design is a direct result of the new findings on digital twins using 6G networks, which reference resiliency and adaptability as AI-controlled management layers [22]. The larger notion of digital twin ecosystems also emphasizes scalability and consistency across system layers, both of which are standard to this architecture [23]. The interpretability focus of feature importance analysis is also consistent with the available literature in the domain of wireless sensor networks, which considers explainable AI as a fundamental demand for reliable anomaly detection in distributed systems [17]. Likewise, decentralization of this framework extension is akin to more recent research on aggregating data in IoT and WSNs, where scaling protocols are the key to detecting anomalies in resource-constrained and massive deployments [16]. This model can be applied to the shift to agentic AI in a wider context, where autonomy in decision-making is seen as a factor of resilience and self-recovery of cyber-physical systems [24]. Collectively, these connections indicate that the proposed architecture is compatible in technical and conceptual ways with emerging concepts of intelligent, quantum-resilient communication infrastructures.

However, this study has some limitations, as it was evaluated in a simulated setting, and although this testbed allowed controlled experimentation and repeatability, it does not yet capture the full complexity of UAV or QKD-based deployments. The analysis was restricted to natural variations in latency and packet loss, without adversarial tests that could directly challenge the SVM classifier or the DQN policy. Moreover, the reinforcement learning model was trained with a limited state space, and the multi-agent evaluation was performed at a relatively small scale, focusing on proof-of-concept validation. These factors point to future research directions, such as adversarial robustness evaluations, broader state modeling, and scalability experiments that involve federated reinforcement learning to coordinate UAV swarms. This outlook is consistent with broader AI risk management perspectives, where the protection of intelligent workloads against adversarial manipulation and their alignment with standardized frameworks are emphasized as critical for the Internet of Robotic Things [25]. However, it should be noted that the edge-deployable design has already identified practical domains of use, including disaster recovery, resource sharing, and secure UAV-based services, which indicates that further refinement could transform the framework into a technically feasible and operationally robust solution.

V. CONCLUSION

The study introduced an AI-based architecture of quantum-secure communication in UAV and edge-based systems to support essential requirements in cryptographic key management and access control. The system proves that it is possible to integrate intelligent decision-making with modular, containerized deployment by using SVM to filter access in real-time and DQN to adaptively rotate encryption keys using Docker, Kubernetes, NS-3, and SimulaQron. The effectiveness of both agents is confirmed by the experimental results: the SVM demonstrated 96.8% accuracy and a recall of 99.2% in the anomalous traffic, whereas the DQN had 92.5% accuracy and stable policy learning across the simulated network conditions. These findings are in accordance with the existing

literature supporting the use of AI to enhance security and offer a practical, testable implementation in the simulation settings. Although hardware deployment in real-time and live integration of QKD is still an objective, the existing framework lays a scalable and flexible foundation of secure, latency-aware communication. The readiness and modularity of the architecture enable it to be critical in the use cases of disaster response, UAV surveillance, and secure autonomous systems. Future work will focus on implementing this system in real-world situations in federated environments and more state inputs to make the policy even more adaptable and intelligent in terms of security.

REFERENCES

[1] P. Bhide, D. Shetty, and S. Mikkili, "Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain," *IET Quantum Communication*, vol. 6, no. 1, 2025, Art. no. e12114, https://doi.org/10.1049/qtc2.12114.

[2] I. Mahmud and A. Abdelhadi, "Artificial Intelligence in Quantum Communications: A Comprehensive Survey," *IEEE Access*, vol. 13, pp. 121174–121205, 2025, https://doi.org/10.1109/ACCESS.2025.3585799.

[3] S. Hashima, A. Gendia, K. Hatano, O. Muta, M. S. Nada, and E. M. Mohamed, "Next-Gen UAV-Satellite Communications: AI Innovations and Future Prospects," *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 1990–2021, 2025, https://doi.org/10.1109/OJVT.2025.3587028.

[4] Y. Sanjalawe, S. Fraihat, S. Al-E'Mari, M. Abualhaj, S. Makhadmeh, and E. Alzubi, "A Review of 6G and AI Convergence: Enhancing Communication Networks With Artificial Intelligence," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 2308–2355, 2025, https://doi.org/10.1109/OJCOMS.2025.3553302.

[5] B. R. Das, S. R. Hasan, S. R. Sabuj, M. A. Hossain, and S. K. Ray, "A Comprehensive Survey on Emerging AI Technologies for 6G Communications: Research Direction, Trends, Challenges, and Opportunities," *International Journal of Intelligent Networks*, vol. 6, pp. 113–150, Jan. 2025, https://doi.org/10.1016/j.ijin.2025.06.001.

[6] A. Alsaeed, S. Almowuena, and A. N. Alyahya, "BAAIoV: A Blockchain-Based Authentication and Authorization Framework for Secure and Reliable Internet of Vehicles Communication," *IEEE Access*, vol. 13, pp. 150821–150837, 2025, https://doi.org/10.1109/ACCESS.2025.3601003.

[7] X. Li, F. Dunkin, and J. Dezert, "Multi-source information fusion: Progress and future," *Chinese Journal of Aeronautics*, vol. 37, no. 7, pp. 24–58, Jul. 2024, https://doi.org/10.1016/j.cja.2023.12.009.

[8] M. Alsader, A. A. Barakabitze, and I. H. Mkwawa, "QoE-Driven Adaptive Video Streaming: Architectures, Techniques, and Future Research Challenges Toward 6G Networks," *IEEE Access*, vol. 13, pp. 157408–157441, 2025, https://doi.org/10.1109/ACCESS.2025.3597058.

[9] M. S. Akbar, Z. Hussain, M. Ikram, Q. Z. Sheng, and S. C. Mukhopadhyay, "On challenges of sixth-generation (6G) wireless networks: A comprehensive survey of requirements, applications, and security issues," *Journal of Network and Computer Applications*, vol. 233, Jan. 2025, Art. no. 104040, https://doi.org/10.1016/j.jnca.2024.104040.

[10] M. Banafaa *et al.*, "6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities," *Alexandria Engineering Journal*, vol. 64, pp. 245–274, Feb. 2023, https://doi.org/10.1016/j.aej.2022.08.017.

[11] S. K. Khan, N. Shiwakoti, A. Diro, A. Molla, I. Gondal, and M. Warren, "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," *International Journal of Critical Infrastructure Protection*, vol. 47, Dec. 2024, Art. no. 100724, https://doi.org/10.1016/j.ijcip.2024.100724.

[12] A. Alhosban, "Binary Offset Carrier (BOC) and Binary Phase Shift Keying (BPSK) Modulation in Indoor Drones GNSS Receivers using Multipath Error Envelope MEE Technique," *International Journal of Membrane Science and Technology*, vol. 10, no. 3, pp. 460–475, Jul. 2023, https://doi.org/10.15379/ijmst.v10i3.1554.

[13] M. I. Khan *et al.*, "Integrating industry 4.0 for enhanced sustainability: Pathways and prospects," *Sustainable Production and Consumption*, vol. 54, pp. 149–189, Mar. 2025, https://doi.org/10.1016/j.spc.2024.12.012.

[14] A. Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, "A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook," *Ad Hoc Networks*, vol. 130, May 2022, Art. no. 102790, https://doi.org/10.1016/j.adhoc.2022.102790.

[15] S. R. Pokhrel, J. Kua, B. Fleming, S. Ozer, J. Howe, and A. Walid, "Multipath TCP implementation under FreeBSD-13 for pluggable machine learning models," *Computer Networks*, vol. 252, Oct. 2024, Art. no. 110671, https://doi.org/10.1016/j.comnet.2024.110671.

[16] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT applications – A comprehensive survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 651–681, Feb. 2023, https://doi.org/10.1016/j.jksuci.2023.01.008.

[17] M. Trigka and E. Dritsas, "Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends," *IEEE Access*, vol. 13, pp. 96365–96399, 2025, https://doi.org/10.1109/ACCESS.2025.3572328.

[18] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 1559–1576, Feb. 2021, https://doi.org/10.1007/s12652-020-02228-z.

[19] S. Ali and B. Djaouida, "Optimizing Quantum Key Distribution Protocols using Decoy State Techniques and Experimental Validation," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15133–15140, Aug. 2024, https://doi.org/10.48084/etasr.7521.

[20] B. M. Mohsen and M. Mohsen, "Intelligent Supply Chain Networks: Integrating AI, Big Data, and Future Communication Technologies for Enhanced Decision-Making," *Procedia Computer Science*, vol. 265, pp. 8–16, Jan. 2025, https://doi.org/10.1016/j.procs.2025.07.150.

[21] S. Krishnan, B. Boroujerdian, W. Fu, A. Faust, and V. J. Reddi, "Air Learning: a deep reinforcement learning gym for autonomous aerial robot visual navigation," *Machine Learning*, vol. 110, no. 9, pp. 2501–2540, Sep. 2021, https://doi.org/10.1007/s10994-021-06006-6.

[22] M. Sheraz, T. C. Chuah, Y. L. Lee, M. M. Alam, A. Al-Habashna, and Z. Han, "A Comprehensive Survey on Revolutionizing Connectivity Through Artificial Intelligence-Enabled Digital Twin Network in 6G," *IEEE Access*, vol. 12, pp. 49184–49215, 2024, https://doi.org/10.1109/ACCESS.2024.3384272.

[23] D. Ivanov, "Conceptual and formal models for design, adaptation, and control of digital twins in supply chain ecosystems," *Omega*, vol. 137, Dec. 2025, Art. no. 103356, https://doi.org/10.1016/j.omega.2025.103356.

[24] S. Hosseini and H. Seilani, "The role of agentic AI in shaping a smart future: A systematic review," *Array*, vol. 26, Jul. 2025, Art. no. 100399, https://doi.org/10.1016/j.array.2025.100399.

[25] H. Karim, D. Gupta, and S. Sitharaman, "Securing LLM Workloads With NIST AI RMF in the Internet of Robotic Things," *IEEE Access*, vol. 13, pp. 69631–69649, 2025, https://doi.org/10.1109/ACCESS.2025.3561235.

AUTHORS PROFILE

Lara Mohammad Hamza Shhab received a B.Eng. degree in Electrical Engineering/Computer from the Jordan University of Science and Technology in 2002, an M.S. degree in Computer and Communication Engineering from UKM, Malaysia, 2005, and a Ph.D. degree in Electrical and Electronics Engineering/Wireless Networks from EMU, North Cyprus, Turkey, 2020. She has been an Assistant Professor at the Faculty of Engineering at Jadara University, Jordan. Then she was a trainer at CISCO Academy in the Vocational Training Corporation in Jordan. Since then, she has been an Assistant Professor in Aviation Maintenance in the Aviation Sciences Faculty, Amman Arab University, Jordan. In addition, she has 9 years of Academic experience before her Ph.D. in computer and communication engineering departments. Her research interests include wireless networks, millimeter

waves, machine learning algorithms associated with wireless techniques, 5G, impulsive noise, privacy, security, and artificial intelligence of wireless networks and aviation systems.

Ahmad Alhosban received a B.Eng. degree in Electrical Engineering/Communications from Mu'tah University, Jordan, in 1994, an M.S. degree in Satellite-Based Communication and Navigation Engineering from ENAC University, France, 2006, and a Ph.D. degree in GNSS Engineering from Ludovika University, Hungary, 2022. Since then, he has been an Assistant Professor in the Department of Aviation Maintenance, Amman Arab University. In addition, he has 25 years of practical experience in both installation and R&D in Navigation and Communication Systems at the Jordanian Air Force. His research interests include Aviation Electronics (Avionics), GNSS, GBAS, GPS, Galileo satellite-based navigation systems, DME, VOR, ILS, ground-based navigation systems, drone communication systems, and artificial intelligence digital instrument systems.