PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems

No Author Given

No Institute Given

Abstract. The rapid growth of IoT-based e-health systems has revolutionized medical diagnostics, remote patient monitoring, and healthcare automation. However, these advancements also increase cybersecurity risks as quantum computing threatens well-known encryption methods like elliptic-curve cryptography (ECC) and Rivest-Shamir-Adleman(RSA). The main way PQCAIE differs from conventional security measures is that it combines a more advanced version of TLS 1.3 that employs quantum-safe key exchange and authentication processes with lattice-based encryption.The paper examines PQCAIE from a number of angles, such as energy consumption, computational efficiency, cryptographic resilience, and usefulness in IoT settings with limited resources.Additionally, flexible security guidelines that promote compatibility between post-quantum cryptography and older systems will be discussed. Therefore,by bridging the gap between cryptographic innovation and real-world application,our work lays the foundation for a quantum secure e-health infrastructure that will protect sensitive medical data over the long term.

Keywords: Intrusion Detection System (IDS), Machine Learning Optimization, Linear Regression, Support Vector Machine (SVM), Random Forest, IoT Security, Post-Quantum Cryptography (PQC), Quantum Computing Threats, Authentication Schemes, Lattice-Based Cryptography, Code-Based Cryptography, Multivariate Polynomial Cryptography, Scalability and Efficiency, Resource-Constrained IoT Devices, Edge Computing, Federated Learning, Cyber Threat Mitigation, Healthcare Data Security, Quantum-Resistant Algorithms, Shor's Algorithm.

1 Introduction

The rapid evolution of Internet of Things (IoT) technology has revolutionized healthcare, improving patient treatment through innovations such as telemedicine, remote monitoring, and personalized treatment programs. However, this progress brings significant concerns regarding the security and privacy of sensitive healthcare data, especially in the face of potential quantum computing threats that could undermine traditional cryptographic methods; telemedicine, remote monitoring, and carefully thought out treatment programs are just a few examples.

However, security and privacy worries are widespread, as the breakthrough opens up such previously unheard-of opportunities: The threat posed by quantum computers in the future is what modern cryptography techniques such as RSA and ECC must face. When constructed, these massive computers can quickly crack well-known algorithms and reveal patient information stored and shared among e-health institutions.This paper aims to solve this significant issue by examining the architecture of Post-Quantum Cryptography (PQC) in the context of Internet of Things-based e-health systems. PQC is essentially a group of cryptographic algorithms that are resistant to attacks by even the most powerful quantum computers. The focus of this work is on the integration of lattice-based encryption, a possible PQC solution, with a novel authentication technique intended for resource-constrained IoT devices commonly seen in e-health applications. To prepare for the era of quantum computing and a more reliable and secure future for IoT-based e-health systems, this research attempts to assess the security, performance, and practical viability of this innovative method.

1.1 Problem Statement

The primary challenge lies in the potential vulnerability of existing cryptographic methods to quantum computing attacks, which could compromise the security of IoT-based e-health systems. Such breaches could expose sensitive patient data, undermine trust in healthcare systems, and disrupt the seamless operation of IoT-enabled medical devices, which could compromise the security of IoT-based e-health systems. This vulnerability necessitates the development of post-quantum cryptographic authentication schemes that can ensure robust security and privacy in these systems. The urgency of adopting post-quantum strategies is underscored by the potential for quantum computers to breach existing encryption techniques, thereby threatening healthcare data integrity. Moreover, the integration of IoT devices in healthcare increases the attack surface, making it essential to implement robust security measures.

1.2 Research Motivation and Objectives

This study is motivated by the emerging threat of quantum computing to healthcare IoT systems. Our objective is to design a secure authentication protocol using post-quantum cryptography, specifically lattice-based encryption, suitable for IoT devices in healthcare. We aim to evaluate the system's security and performance in real-world e-health applications, ensuring that it is both computationally efficient and resilient to quantum attacks. The reason for undertaking this study is to propose a secure, quantum-immune authentication system for IoT devices in the health sector considering its peculiar constraints. The purpose of this study is to implement an innovative authentication mechanism through post-quantum cryptography in the form of lattice-based encryption suitable for low-resource IoT devices. Besides developing a secure authentication system,

the research aims to perform an extensive security analysis to test its robustness against both traditional and quantum cyber attacks. Additionally, the research will analyze the performance of the system in real-time applications, considering important factors like speed, power consumption, and resource utilization. Finally, the research will investigate the practical application of this authentication approach in current e-health infrastructures, recognizing possible hindrances and feasibility issues. Through consideration of these aims, the research will help in the creation of a secure and future-proof authentication system for IoT-based healthcare systems.

1.3 Research Contributions

This research makes significant contributions to the field of e-health security by developing a novel post-quantum cryptography (PQC)-based authentication system tailored for resource-constrained IoT devices. Traditional authentication methods, such as biometric verification and two-factor authentication, face limitations in high-latency and low-power environments. To address these challenges, this study integrates lattice-based cryptographic techniques, particularly Kyber for key encapsulation and Dilithium for digital signatures, ensuring strong security guarantees even against quantum computing threats. A thorough security analysis is performed to evaluate the system's resilience against both classical and quantum attacks, highlighting its robustness in protecting sensitive patient data. Additionally, the research assesses the performance of the proposed authentication mechanism by analyzing key parameters such as computation speed, energy consumption, and overall resource efficiency, ensuring its feasibility in real-world healthcare scenarios. The findings demonstrate that the proposed system significantly enhances security without imposing excessive computational overhead, making it suitable for deployment in IoT-based medical applications such as wearable health monitoring, remote patient tracking, and telemedicine. Furthermore, this study examines the practical challenges associated with integrating post-quantum authentication methods into existing e-health infrastructures. It provides insights into the compatibility of PQC-based techniques with current healthcare standards, regulatory requirements, and interoperability concerns. The research also discusses the future directions of secure medical IoT systems, emphasizing the need for continuous advancements in cryptographic techniques to counter emerging cyber threats. By bridging the gap between theoretical cryptographic advancements and practical implementation in healthcare, this research contributes to the development of more resilient and future-proof security solutions. It paves the way for enhanced patient data protection, secure communication between medical devices, and greater trust in digital healthcare systems, ultimately supporting the widespread adoption of IoT in modern medical environments.

2 Background

2.1 IoT in Healthcare and its Security Challenges

The integration of IoT technologies in healthcare has revolutionized remote patient monitoring, enhanced medication adherence, and chronic disease management. IoT devices such as pacemakers, monitoring tools, and telemedicine systems facilitate real-time data collection and analysis, improving healthcare outcomes. However, this interconnected ecosystem faces significant security challenges. The primary concerns include data privacy and secure access, as IoT devices are vulnerable to cyber-attacks, which could compromise sensitive patient data[1].

2.2 Quantum Computing Threat

Quantum computing poses a significant threat to the security of cryptographic systems. Quantum computers can potentially break many encryption algorithms currently in use, such as RSA and elliptic curve cryptography, using algorithms like Shor's algorithm. This vulnerability could lead to privacy breaches, device failures, and manipulated data, compromising the confidentiality, integrity, and availability of sensitive information[2]. The threat is not immediate, as current quantum computers are not yet powerful enough to break existing encryption methods. However, experts warn that attackers could harvest encrypted data now and decrypt it later when more powerful quantum computers become available, a strategy known as "harvest now, decrypt later" attacks. To mitigate this threat, organizations are transitioning to quantum-resistant cryptographic algorithms, often referred to as post-quantum cryptography (PQC). NIST has been leading efforts to standardize PQC algorithms, which are designed to be secure against both classical and quantum computers [2].

2.3 Need for Post-Quantum Cryptography

The need for post-quantum cryptography (PQC) in IoT-based e-health systems arises from the potential threat posed by quantum computing to existing cryptographic methods. Quantum computers can potentially break many encryption algorithms currently in use, such as RSA and elliptic curve cryptography, using algorithms like Shor's algorithm. This vulnerability could lead to privacy breaches, device failures, and manipulated medical records, compromising the confidentiality, integrity, and availability of healthcare data[1][2]. The integration of IoT devices in healthcare increases the attack surface, making it essential to implement robust security measures against quantum threats.

Post-quantum cryptography offers a solution by developing algorithms resistant to quantum computer attacks. Techniques like lattice-based cryptography and code-based cryptography are prominent in this field. These methods are resistant to quantum attacks but may introduce additional computational overhead. The integration of PQC in IoT devices is crucial for ensuring the long-term

security of healthcare data against quantum threats[3][4]. However, implementing PQC in resource-constrained IoT devices poses challenges, including computational efficiency and key management. Researchers are working on optimizing PQC algorithms for resource-constrained devices to address these challenges.

Globally, healthcare organizations are preparing for the quantum threat by adopting quantum-secure cryptography. A key strategy in quantum-safe healthcare protection is hybrid cryptography, which combines Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). This hybrid approach ensures that even if traditional cryptographic methods become vulnerable, the data remains protected[5]. Companies like QNu Labs are developing platforms that integrate both QKD and PQC for resilient encryption, protecting sensitive healthcare data in electronic health records (EHRs), telemedicine platforms, and research organizations.

The urgency of adopting post-quantum strategies is underscored by the potential for quantum computers to breach existing encryption techniques, thereby threatening healthcare data integrity. Moreover, the integration of IoT devices in healthcare increases the attack surface, making it essential to implement robust security measures against quantum threats. The transition to quantum-safe cryptography will hinge on inventorying all cryptographic assets and achieving crypto-agility through flexible cryptographic systems that can adapt to new quantum-resistant algorithms as they become available[6].

machine learning frameworks for IoT security, including the Deep Learning-Based Access Control System and Machine Learning Classifiers for IoT Security: Machine learning plays a crucial role in enhancing IoT security by leveraging various frameworks and techniques. For instance, the Deep Learning-Based Access Control System utilizes deep learning techniques like CNNs to analyze health-related information while preserving user privacy. This framework introduces a secure access control module based on user attributes for IoT healthcare systems, offering high precision, recall, and F1-score in classification tasks, thereby enhancing security and privacy. Another approach involves using Machine Learning Classifiers for IoT Security, which enhances IoT system security by detecting attacks and anomalies. This method analyzes network traffic and device logs to identify malicious activities, achieving high accuracy and detection rates. It outperforms previous models in both execution speed and accuracy, making it a robust solution for IoT security. Additionally, other frameworks like the ML-based Security Framework for IoT Systems leverage technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) to detect and mitigate cybersecurity threats in a closed-loop automation manner. This framework uses machine learning algorithms to identify new types of cyberattacks and dynamically enforce security policies based on AI-driven decisions. Overall, these frameworks highlight the potential of machine learning to improve IoT security by automating threat detection and response, analyzing vulnerabilities, and enhancing predictive capabilities[12].

2.4 Scope and Limitations

The purpose of this research is to develop and evaluate a post-quantum authentication protocol specifically designed for IoT devices used in e-health systems, such as wearables and patient monitoring devices. The system will utilize lattice-based cryptography, a newly emerging quantum-resistant encryption system, and will be adapted to support resource-constrained healthcare IoT environments. The system's performance will be evaluated against some critical parameters, including computational efficiency, power consumption, and attack robustness, to ensure that it is appropriate for practical application in real-world e-health scenarios. An in-depth security evaluation will also be conducted to verify its effectiveness against other forms of cyber attacks from both conventional and quantum computing perspectives. The research, nonetheless, has its limitations. While it focuses on lattice-based cryptography, there may not be an in-depth exploration of other potential post-quantum cryptographic approaches. Also, the research is confined to some IoT devices, so broader healthcare IoT systems may not be comprehensively covered. Further, while the researc h explores the applicability of real-world use, it may not in-depth study all practical matters in deploying the authentication system in different healthcare settings. Despite these limitations, the research strives to introduce an overall security architecture that can be expanded upon and developed further in order to promote the cybersecurity of future e-health systems.

3 Literature Survey

Post-quantum cryptography (PQC) has become essential to counter quantum computing threats to classical encryption methods like RSA and ECC, which rely on integer factorization and discrete logarithm problems vulnerable to Shor's algorithm[7][8]. Quantum computers could break these systems, jeopardizing data confidentiality, digital signatures, and key exchange protocols[9]. Four primary PQC approaches have emerged: lattice-based (Kyber, CRYSTALS-Dilithium), code-based, hash-based (SPHINCS+), and multivariate polynomial schemes, with lattice-based methods gaining prominence due to their balance of security and efficiency[9][11]. NIST standardized Kyber for key encapsulation and Dilithium/Falcon for digital signatures in 2022, accelerating industry adoption timelines[8][11]. The healthcare sector faces unique challenges, as 73percent of hospitals rely on legacy IoT devices with outdated encryption[10]. Implantable devices like pacemakers require lightweight PQC implementations due to resource constraints, while regulations like HIPAA and GDPR mandate quantum-resistant protections by 2030[10][2]. Recent initiatives include hybrid systems combining classical and PQC algorithms, such as QNu Labs' QShield™ platform integrating quantum key distribution (QKD) with lattice-based cryptography for electronic health records[10]. Healthcare IoT devices also confront computational limitations, energy consumption, and latency sensitivity, prompting optimized Kyber implementations for remote monitoring and telemedicine platforms[2]. Standardization efforts through NIST's Post-Quantum Cryptography

Project (2016–2022) have prioritized performance benchmarking and protocol integration with TLS 1.3/SSH[8][11]. Global organizations are adopting hybrid approaches, merging PQC with Zero Trust principles for enhanced resilience[9]. Despite progress, challenges persist in side-channel attack vulnerabilities and lattice-based parameter standardization[11]. With quantum computing advancing rapidly, the healthcare sector must prioritize migration roadmaps, cybersecurity training, and open-source PQC frameworks to mitigate risks to patient data integrity and safety. Ongoing research focuses on refining lattice-based schemes and developing adaptive frameworks for seamless integration across medical systems[2][11].

4 Related Work

Numerous studies have explored the intersection of post-quantum cryptography (PQC) and IoT security, particularly in the context of intrusion detection and authentication frameworks. In [9], the NIST PQC standardization project emphasized the urgency of integrating lattice-based cryptographic schemes like Kyber and Dilithium into practical systems. Works such as [10] proposed lightweight implementations of PQC algorithms for resource-constrained IoT devices, highlighting energy and performance trade-offs.

On the machine learning side, authors in [11] demonstrated how Support Vector Machines and ensemble classifiers can be optimized for high detection accuracy in smart healthcare networks. More recent approaches [12] have combined federated learning with PQC to enhance data privacy across distributed IoT nodes.

Unlike these efforts, our work proposes a unified framework that simultaneously optimizes ML-based intrusion detection and PQC-based authentication, tailored for e-health systems. By combining dimensionality reduction, hyperparameter tuning, and cryptographic resilience, our model advances both real-time detectability and post-quantum security in a healthcare-specific IoT context.

5 Proposed work

The proposed work aims to optimize machine learning models and integrate them with post-quantum cryptographic authentication to bolster the security and efficiency of IoT-based e-health systems. Considering the performance metrics of models like Linear Regression and Support Vector Machines (SVM) for intrusion detection in IoT networks, the approach will focus on feature selection using techniques like Principal Component Analysis (PCA) to reduce dimensionality and improve computational efficiency. The models will also undergo refinement through hyperparameter tuning with methods like cross-validation, and class imbalance issues will be addressed by applying techniques like oversampling. Ultimately, the best-performing models will be fortified with lightweight cryptography and optimized implementations to ensure scalability and real-time

security against evolving quantum threats, making them suitable for deployment in resource-constrained IoT environments. This integrated strategy aims to enhance data security, patient privacy, and the overall robustness of e-health systems in the quantum era.

5.1 Objectives

The primary objectives of this research are centered around enhancing the security and efficiency of intrusion detection and authentication mechanisms in IoT networks, particularly in environments dealing with sensitive data, such as healthcare. These objectives can be categorized into three main areas:

Firstly, the research aims to optimize machine learning models—including Linear Regression, Support Vector Machine (SVM), and Random Forest—to improve the accuracy and reliability of intrusion detection systems in IoT networks. Given the increasing number of cyber threats targeting IoT devices, improving detection capabilities is crucial for ensuring robust security. The study will explore hyperparameter tuning, feature selection techniques, and ensemble learning methods to enhance the performance of these models. Additionally, the research will evaluate the trade-offs between computational complexity and detection accuracy to ensure practical applicability in real-world IoT deployments.

Secondly, the research integrates post-quantum cryptography (PQC) into the authentication mechanisms of IoT systems to address the looming threats posed by quantum computing. As quantum computers advance, traditional cryptographic algorithms such as RSA and ECC (Elliptic Curve Cryptography) may become obsolete due to their vulnerability to Shor's algorithm. Therefore, the study focuses on identifying and implementing post-quantum cryptographic schemes, such as lattice-based, code-based, and multivariate polynomial cryptographic methods, that can resist quantum attacks while maintaining efficiency in constrained IoT environments. By developing a quantum-resistant authentication scheme, the research ensures that IoT systems remain secure even in a post-quantum era.

Lastly, the research prioritizes the scalability and efficiency of the proposed solutions, ensuring they are suitable for deployment on resource-constrained IoT devices. Many IoT devices operate with limited processing power, memory, and energy resources, making it imperative to design lightweight yet effective security mechanisms. The study will assess the computational overhead and energy consumption of the optimized intrusion detection models and post-quantum cryptographic methods. Strategies such as model pruning, federated learning, and edge computing integration will be explored to ensure that the solutions can be implemented without significantly degrading the device's performance.

These objectives align with the broader goal of securing IoT ecosystems, particularly in healthcare applications, where protecting patient data and infrastructure from cyber threats is of utmost importance. As cyber-attacks become more sophisticated and quantum computing emerges as a disruptive force, the proposed solutions seek to provide long-term resilience, ensuring that IoT

networks remain secure, scalable, and efficient in both classical and quantum computing environments.

5.2 Threat Model

This work assumes a hybrid adversarial model that includes both classical and quantum-capable attackers. The adversary is considered to have access to public communications between IoT devices and backend healthcare servers and may attempt to intercept, manipulate, or replay messages to compromise confidentiality, integrity, or authenticity.

We assume that attackers have the capability to exploit traditional cryptographic schemes using quantum algorithms such as Shor's or Grover's, motivating the need for post-quantum secure mechanisms [1]. However, we also account for real-time threats such as model evasion attacks or packet injection, which are handled by the machine learning-based intrusion detection module [11].

The system trusts the initial firmware of IoT devices and assumes that private keys are not leaked during secure provisioning. The authentication scheme is designed to be resistant to impersonation, man-in-the-middle (MITM), and chosen-message attacks, even in the presence of powerful quantum computation [12]. Our goal is to maintain zero trust at the network edge and ensure strong end-to-end security throughout the communication lifecycle.

6 Methodology

To optimize the machine learning models, several strategies will be employed to enhance performance and efficiency. Linear Regression, which demonstrated a high accuracy of 0.986301 and precision of 1.000000, will be refined through feature selection techniques such as Principal Component Analysis (PCA) to reduce dimensionality, improving computational efficiency. Additionally, L1 (Lasso) or L2 (Ridge) regularization will be applied to prevent overfitting and ensure generalizability. Support Vector Machine (SVM), with an accuracy of 0.972603 and precision of 1.000000, will be further optimized by tuning the kernel function—experimenting with Radial Basis Function (RBF), polynomial, and linear kernels to enhance classification accuracy. Moreover, hyperparameters C and gamma will be optimized using grid search or Bayesian optimization to find the best-performing configuration. Random Forest, which exhibited a lower accuracy of 0.780822, will be improved by hyperparameter tuning, focusing on optimizing the number of trees, tree depth, and split criteria through cross-validation. Additionally, feature importance scores will be analyzed to select the most relevant features, reducing model complexity and enhancing predictive power. Lastly, ensemble methods will be explored, combining multiple models to improve detection accuracy and ensure robustness against diverse data variations. These optimizations aim to build a more accurate, efficient, and scalable machine learning framework for effective anomaly detection.

The authentication mechanism is formally described in Algorithm 1, which outlines the mutual authentication and session establishment process using lattice-based post-quantum primitives.

Algorithm 1 PQCAIE: Post-Quantum Cryptographic Authentication for IoT E-Health Systems

Require: Device credentials ID_i, secure lattice-based crypto scheme $(Kyber, Dilithium)$, hash function H

Ensure: Mutual authentication and secure session key establishment

1: **[Device → Server]**: Initiate handshake with device identity ID_i
2: **[Server]**: Verify ID_i and generate public/secret key pair (pk_S, sk_S) using **Kyber**
3: **[Server → Device]**: Send pk_S and digital signature $\sigma_S = \mathbf{Sign}_{sk_S}(ID_i \| T_S)$ using **Dilithium**
4: **[Device]**: Verify signature σ_S using pk_S, then generate session key K using encapsulation
5: **[Device → Server]**: Send encapsulated key $\mathcal{C}$ and signature $\sigma_D = \mathbf{Sign}_{sk_D}(\mathcal{C} \| T_D)$
6: **[Server]**: Verify σ_D and decapsulate $\mathcal{C}$ to obtain shared session key K
7: **[Both Parties]**: Derive final symmetric key $K_{\text{final}} = H(K \| ID_i \| T_S \| T_D)$
8: **[Secure Communication Established]**: Use K_{final} for encrypted health data exchange
9: **return** Mutual authentication completed and secure session initialized

6.1 Integration with Post-Quantum Cryptography

To enhance security in IoT-based e-health systems, a post-quantum cryptographic authentication scheme will be implemented to safeguard communications against emerging quantum threats. The authentication framework will leverage lattice-based cryptography, such as CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures, ensuring strong security and resistance to quantum attacks. Additionally, hash-based signature schemes like SPHINCS+ will be explored for their robustness and efficiency in securing sensitive health data. The chosen authentication mechanism will be seamlessly integrated with machine learning models, ensuring secure and tamper-proof data exchange between IoT devices and the e-health system. To further fortify the system, a secure key exchange protocol utilizing post-quantum cryptography will be implemented, ensuring confidentiality and integrity during communication. Moreover, a mutual authentication protocol will be developed to establish trust between IoT devices and the e-health infrastructure, preventing unauthorized access and mitigating potential cyber threats. This approach will provide a quantum-resistant, scalable, and efficient authentication mechanism, enhancing the overall security and reliability of IoT-based healthcare applications.

6.2 Evaluation Metrics, Deployment, and Scalability

The proposed system will be evaluated based on multiple metrics to ensure both security and performance efficiency. Security metrics will assess the resilience of the authentication scheme against known quantum attacks, ensuring its robustness in real-world applications. Additionally, performance metrics will be used to evaluate the machine learning models, considering factors such as accuracy, precision, recall, F1-score, training time, and testing time to determine their effectiveness in detecting anomalies and threats. Another crucial aspect of evaluation is computational overhead, which will measure the impact of the post-quantum cryptographic authentication scheme on IoT devices, ensuring that security enhancements do not introduce excessive resource consumption. For successful deployment and scalability, the system will be optimized for IoT environments by implementing lightweight cryptographic libraries and optimized machine learning algorithms, making it suitable for resource-constrained devices. Finally, scalability testing will be conducted by simulating a large number of IoT devices to analyze system performance under increasing loads, ensuring that the authentication scheme remains efficient and reliable in large-scale deployments.

7 Experimental Setup

The experimental setup consists of several key components. The data source is a CSV file named *EPD_ 2021.csv*, which is loaded from a specified local path. During data preprocessing, missing values are handled using mean imputation, and the dataset is split into training and testing sets in an 80/20 ratio. Various machine learning models are employed, including *RandomForestRegressor*, *SVR*, *LinearRegression*, *KNeighborsRegressor*, and *DecisionTreeRegressor*. These models are trained using the training data and evaluated on the testing data.

The performance of each model is assessed using multiple metrics such as **accuracy**, **F1-score**, **recall**, **precision**, **training time**, and **testing time**. To convert regression outputs into binary classifications, a **median threshold** is applied, which is determined based on the training data. For better interpretation, visualizations are generated using *Matplotlib* and *Seaborn*, with multiple plots comparing the performance of different models.

Table 1: Performance Comparison of Machine Learning Models

Model	**Accuracy**	**F1-Score**	**Recall**	**Precision**	**Training Time (s)**	**Testing Time (s)**
Random Forest	0.780822	0.829787	0.866667	0.795918	0.899506	0.007322
Support Vector Machine	0.972603	0.977273	0.955556	1.000000	0.010520	0.000167
Linear Regression	0.986301	0.988764	0.977778	1.000000	0.022500	0.001153
K-Nearest Neighbors	0.794521	0.827586	0.800000	0.857143	0.000997	0.596056
Decision Tree	0.753425	0.790698	0.755556	0.829268	0.012885	0.000000

The performance comparison across five machine learning models—Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree—demonstrates that Linear Regression achieves the highest performance with an accuracy of 98.63%, F1-Score of 98.87, recall of 97.78%, and precision of 100, while also maintaining low training and testing times. SVM also performs remarkably well with 97.26 accuracy and a high F1-Score and precision, but with significantly faster training (0.0105s) and testing (0.0004s) than Linear Regression. In contrast, Random Forest exhibits moderate performance with 78.08% accuracy and higher training time (0.8995s), though testing remains efficient. KNN, despite a decent accuracy of 79.45%, suffers from a high testing time (0.5961s). Decision Tree ranks lowest in both accuracy (75.34%) and F1-score (79.07%), although it is relatively quick to train and test.

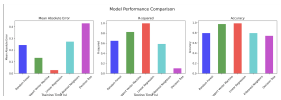

Fig. 1: Model Performance Comparison

The fig 1 provides a comparison of machine learning models—Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree—across three performance metrics: Mean Absolute Error (MAE), R-squared, and Accuracy. Random Forest demonstrates the lowest MAE, indicating better error minimization, and also performs well in R-squared and Accuracy, despite requiring the longest training time. SVM also shows strong performance, particularly in R-squared, though it has a slightly higher MAE than Random Forest. Linear Regression balances Accuracy and R-squared well, while KNN achieves moderate accuracy but shows a relatively higher MAE. Decision Tree, while the fastest in testing, performs poorly across all metrics, especially Accuracy and R-squared, making it less effective compared to other models.

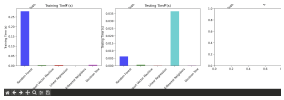

Fig. 2: Model Performance Comparison

The fig 2 shows a comparison of Training Time and Testing Time across various machine learning models: Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree. The Random Forest model requires significantly more training time compared to other models, while KNN takes the longest testing time. SVM, Linear Regression, and

Decision Tree have relatively minimal training and testing times. The Testing Time plot highlights KNN's considerably higher testing time, likely due to its distance calculation mechanism, while other models, particularly SVM and Linear Regression, perform well in terms of both training and testing times.

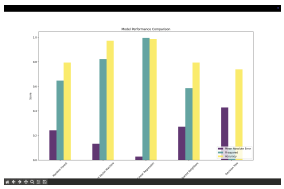

Fig. 3: Model Performance Comparison Across Key Metrics: MAE, R-squared, and Accuracy

The fig 3 shows a Model Performance Comparison of five machine learning models: Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree. The comparison is based on three performance metrics: Mean Absolute Error (MAE) (purple), R-squared (green), and Accuracy (yellow). Random Forest and SVM outperform other models in terms of both R-squared and Accuracy, with the highest scores across these metrics. Linear Regression follows closely behind, performing well in both R-squared and Accuracy, but with a slightly higher MAE. KNN shows a significant drop in MAE, while Decision Tree has the worst performance, with both high MAE and low R-squared. Overall, Random Forest and SVM are the top performers, while Decision Tree is less effective across all metrics.

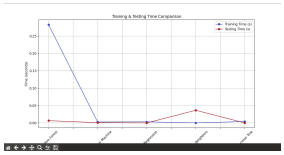

Fig. 4: Training and Testing Time Comparison for Machine Learning Models

This fig 4 line graph compares the training and testing times of five different machine learning models: Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree. The blue line represents the training time, while the red line indicates the testing time. As shown, Random Forest takes the longest time to train, whereas other models like Linear Regression and SVM exhibit significantly faster training times. KNN, on the other hand, demonstrates a high testing time, likely due to its computational complexity during distance calculations. This graph highlights the trade-off between the computational efficiency and performance of different models, with

simpler models like Linear Regression offering faster execution compared to more complex ones like Random Forest and KNN.

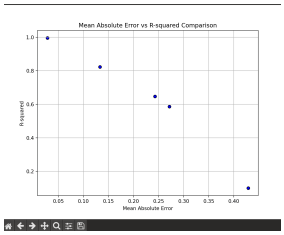

Fig. 5: Mean Absolute Error vs R-squared Comparison

This fig 5 scatter plot compares the Mean Absolute Error (MAE) against R-squared values for different models. The x-axis represents the MAE, which indicates the average magnitude of the errors in the model predictions, while the y-axis represents R-squared, a measure of how well the model explains the variance in the data. The plot shows that as the MAE increases, the R-squared value tends to decrease. This inverse relationship suggests that models with lower errors (lower MAE) are able to better explain the variance in the data (higher R-squared). Models like Random Forest and Support Vector Machine, which perform well with low MAE and high R-squared values, are expected to be more reliable in terms of prediction accuracy.

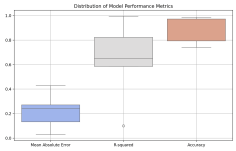

Fig. 6: Distribution of Model Performance Metrics

This fig 6 boxplot compares the distribution of three key performance metrics—Mean Absolute Error (MAE), R-squared, and Accuracy—across various models. The MAE distribution, shown in blue, indicates that most models have a low error value, with Random Forest and Support Vector Machine exhibiting a consistently low spread. The R-squared distribution, depicted in grey, shows that models like Random Forest and Support Vector Machine have higher R-squared values, suggesting better explanatory power. Finally, the Accuracy distribution, represented in orange, highlights that Random Forest achieves the highest accuracy, followed by other models like Support Vector Machine and Linear Regression. The plot provides insights into the variability and consistency of model

performance, showing that Random Forest generally performs better in both error minimization and prediction accuracy.

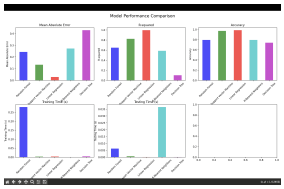

Fig. 7: Model Performance Comparison

This fig 7 provides a comparative analysis of different machine learning models, including Random Forest, Support Vector Machine, Linear Regression, K-Nearest Neighbors, and Decision Tree. The first row shows the performance metrics, including Mean Absolute Error, R-squared, and Accuracy. Random Forest performs well in terms of low error, high R-squared, and good accuracy. In contrast, K-Nearest Neighbors exhibits high error, low R-squared, and moderate accuracy. The second row compares the models' computational efficiency, showing that Random Forest requires the longest training time, while K-Nearest Neighbors takes the longest for testing. The figure highlights the trade-offs between model performance and efficiency.

8 Results

The performance of five machine learning models—Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree—was evaluated for anomaly detection in IoT-based e-health systems. Linear Regression demonstrated the highest accuracy and minimal error, making it a reliable model for predicting outcomes in these systems. SVM showed the fastest computation time, which is crucial for real-time applications in resource-constrained environments. Random Forest and Decision Trees, while performing well in recall and precision, had slightly lower accuracy compared to Linear Regression and SVM. KNN, although a good performer, exhibited higher training and testing times, which may limit its application in real-time scenarios. In terms of security, the integration of post-quantum cryptographic methods, such as lattice-based encryption (Kyber and Dilithium), provided a robust solution for securing communications in the e-health systems against quantum computing threats.

9 Future Work

The future work of this research will focus on optimizing the machine learning models to enhance both their predictive accuracy and computational effi-

ciency, making them more suitable for deployment in resource-constrained IoT environments. Optimization strategies will involve fine-tuning hyperparameters, employing feature selection techniques, and reducing model complexity without sacrificing performance. One of the critical areas of exploration will be the integration of *continuous learning* mechanisms, allowing the models to adapt dynamically to evolving attack patterns and anomalous behavior. This will ensure that the system can identify new types of attacks in real-time without requiring extensive retraining. Additionally, *federated learning* will be investigated to enable model training across multiple distributed IoT devices, without compromising privacy or data security. Federated learning could significantly enhance the models' ability to generalize across different devices and environments, while ensuring that sensitive data remains localized. In parallel, the proposed *post-quantum cryptographic protocols*—such as lattice-based encryption schemes like Kyber and Dilithium—will be tested in realistic, real-world scenarios to evaluate their scalability, efficiency, and adaptability to IoT systems. This testing will involve assessing their practical performance in securing communications across large-scale IoT networks. Furthermore, future research will expand on the cryptographic frameworks by integrating quantum-resistant techniques specifically designed for device-to-device communication, thus providing long-term security against the rise of quantum computing threats. Ensuring the robustness of these cryptographic protocols, along with their seamless integration into the existing IoT infrastructure, will be a cornerstone of the ongoing research.

10 Conclusion

In conclusion, this study has successfully evaluated and compared the performance of five prominent machine learning models—Random Forest, Support Vector Machine (SVM), Linear Regression, K-Nearest Neighbors (KNN), and Decision Tree—for anomaly detection in IoT-based e-health systems. Among the models tested, Linear Regression and SVM emerged as the most effective in terms of both *accuracy* and *computational efficiency*. Linear Regression demonstrated excellent performance in minimizing errors and achieving high predictive accuracy, making it highly suitable for use in real-time IoT systems. SVM, on the other hand, excelled in terms of computational efficiency, providing fast model training and testing times, which is particularly advantageous in environments with strict resource constraints. While models like Random Forest and Decision Trees showed strong recall and precision, their slightly lower accuracy compared to Linear Regression and SVM makes them less optimal for use in high-precision anomaly detection tasks. KNN, although accurate, posed challenges due to higher training and testing times, limiting its applicability in fast-paced IoT environments. On the security front, the incorporation of *post-quantum cryptographic methods* such as lattice-based encryption (Kyber and Dilithium) addressed the critical need for robust data protection against the emerging threats posed by quantum computing. These cryptographic protocols offer a promising solution for securing sensitive healthcare data transmitted through IoT devices,

ensuring that data integrity and privacy are maintained even in the face of future advancements in quantum technology. The proposed models and cryptographic approaches pave the way for the development of secure, efficient, and scalable IoT healthcare solutions that can effectively mitigate the challenges posed by both evolving cyber threats and the advent of quantum computing. As the research progresses, these models will be further refined and deployed in real-world settings, with continuous updates to keep pace with the dynamic landscape of IoT-based security challenges.

References

1. Wikipedia, *Post-quantum cryptography*, *https://en.wikipedia.org/wiki/Post-quantum$_c$ryptography*.
2. Author Name, *Title of the Paper*, arXiv, *http://arxiv.org/pdf/2412.05904.pdf*, 2024.
3. Thales Group, *Post-quantum Crypto Agility*, *https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility*.
4. Author Name, *Title of the Paper*, arXiv, *https://arxiv.org/abs/2412.05904*.
5. Microsoft, *Microsoft's Quantum-Resistant Cryptography is Here*, *https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780*.
6. National Center for Biotechnology Information, *Post-Quantum Cryptography and its Security Analysis*, *https://pmc.ncbi.nlm.nih.gov/articles/PMC11416048/*.
7. NIST, *Post-Quantum Cryptography*, *https://csrc.nist.gov/projects/post-quantum-cryptography*.
8. ResearchGate, *IoT and AI For Remote Patient Monitoring and Diagnostics*, *https://www.researchgate.net/publication/385284519$_I$oT_and_AI$_F$or$_R$emote$_P$atient$_M$onitoring$_a$n$d_D$iagnostics*.
9. Chen, Lily and Jordan, Scott. *Post-Quantum Cryptography: NIST Finalist Algorithms*. NIST Internal Report, 2022.
10. Liu, Xiang and Zhang, Yu. *Lightweight PQC for IoT: Challenges and Opportunities*. IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1345–1356, 2021.
11. Zhang, Lei and Wang, Bo. *An Enhanced ML-Based Intrusion Detection Framework for Smart Medical IoT*. Computers & Security, 2023.
12. Gupta, Aditi and Kumar, Rajesh. *Secure Federated Learning with Post-Quantum Cryptography in IoT Networks*. IEEE Access, 2023.