International Journal of Innovative Research in Engineering
Volume 7, Issue 2 (March - April 2026), PP: 165-171.
https://www.doi.org/10.59256/ijire.20260702021
www.theijire.com
ISSN No: 2582-8746

Develop a secure communication protocol for quantum safe cryptographic systems

Vuta Venkata Suresh[1], Yakkala Damesh[2], Dr. D. Sudha[3]
[1,2,3] *Department of CSE, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.*

How to cite this paper:
Vuta Venkata Suresh [1], Yakkala Damesh [2], Dr. D. Sudha[3], "Develop a secure communication protocol for quantum safe cryptographic systems", IJIRE-V7I2-165-171.

Abstract: *Quantum cryptography is based on quantum mechanics concepts such as superposition and entanglement to provide the inadmissibility of security in communications protocols. It is the purpose of this project to create a safe banking system to trade ships and import-export using the integration of quantum-safe communication protocols and biometric authentication. Through Quantum Cryptographic System and Blockchain protocols (RSA and SHA 256), the platform can guarantee that it controls data transfer safely and detects any form of unauthorized interception. UPI transactions with an added security of verifying the identity of the users are implemented through face recognition. Furthermore, goods and services control to the encryption system to entrepreneurs are combined to render all the communications to be resistant to classical and other quantum based attacks. This system will address the cybersecurity issues that are related to the high-value transaction to offer a strong solution to ensure the safety of data transmission and authentication. This not only gives a more powerful security to online financial transactions, but also the long-term security against the evolving cyber threats. With quantum cryptography integrated, the system is in a good position to overcome the challenges posed by the development of quantum computing. In the end, this project becomes a new norm in the banking and financial fields in regards to safe high stakes transactions.*

Keywords: *Quantum Cryptography, Quantum-Safe Communication Protocols, Biometric Authentication, RSA encryption, SHA 256, Block chain Technology, Face Recognition, UPI Transactions, Secure Data Exchange, Cyber-Security, Quantum Computing, Financial Transaction, Secure Banking Platform, Ship Trading, Import Export.*

I.INTRODUCTION

In the online era, the security of confidential data, particularly in the banking industry, is a matter of concern. As the world becomes highly technological, the famous encryption systems like RSA and AES are more prone to an attack, particularly the upcoming technologies like quantum computing. One possible answer to that question would be quantum cryptography, based on a few principles of quantum mechanics like superposition and entanglement, to produce communication protocols that are theoretically impossible to break. The project is concerned with the design of a safe communication system which will employ quantum-safe cryptography to deal with the growing threats that arise due to the rise of quantum computing to the current cryptographic system.The project is linked to the development of a safe banking system that will adopt quantum safe cryptography to carry out the high risk banking transactions in ship trading and import export business. Since such transactions that involve large amounts of money and sensitive information are of high importance, the integrity and confidentiality of all communications should be considered paramount. This platform will provide a secure platform by integrating quantum-safe cryptographic algorithms (e.g., RSA, SHA-256) and biometric sign-in to provide a robust security system that can withstand both classical and quantum-based cyber-attacks.

Besides quantum safe cryptography, biometric authentication,e.g. face recognition, is also present in the platform in Unified Payments Interface (UPI) transactions. Face recognition is a significant added security as we would wish to be assured that only authorized persons can make transactions particularly in high value transactions. The quantum-resistant encryption algorithms used with the blockchain technology help to send and store all the information related to the transactions in a safe manner and in the case of the interception or manipulation of the data, it will be noticed in real-time. This quantum safe cryptography or biometric authorization is a novel method of ensuring the safety of online financial transactions.With the global confronted with the increased number of cyber threats, including the challenges of quantum computing systems, the project is a brilliant idea that does not only address the current cyber security weakness of the present but also equips the system with the demands of the future. The system is also properly equipped with quantum cryptography, which means that the system is capable of offering long-term security to sensitive financial transactions, which can be viewed as a road map of the future of secure communication in the banking and financial sectors. The resultant agenda is to develop a new norm of the high-value, high-stakes transactions to ensure that the security of the users and businesses now and in the future is guaranteed.

II.LITERATUTRE REVIEW

In the modern digital environment, the security of sensitive financial transactions is one of the most topical problems. With the world becoming more dependent on the digital platform and banking, trade and communications, the weakness of current cryptography systems becomes even more evident. The current encryption algorithms, including RSA and AES, have been endangered by the development of quantum computing, and this fact represents an existential danger to the existing encryption algorithms. This is especially alarming in the highly prized industries like banking where a breach would be disastrous to the world economies and the lives of individuals. As the field of quantum computing continues to advance at a very alarming rate, the necessity of having safe communication systems that can resist all both classical and quantum-related attacks has never been more urgent.

This is the issue that the project plans to deal with through the creation of a secure banking platform that incorporates quantum-safe cryptographic systems. This platform shall be in such a way that it protects the ship trading and import-export businesses- industries where high-stakes financial transactions are involved. Using quantum-resistant algorithms such as RSA, SHA-256 and blockchain, the platform will be able to make all communications secure even during the possible quantum-related attacks. Besides these quantum-safe protocols, biometric authentication (face recognition) also enhances the safety of the platform, as the presence of an extra step in verifying the identity of high-value transactions (like UPI payment) can be introduced.

Nevertheless, the actual efficiency of a security system cannot be evaluated only by the capability to prevent illegal access but also by the capability to identify and react to the possible threats in real-time. Artificial intelligence-based predictive systems have the potential to increase the level of security through real-time surveillance, notices, and practical information. When applied to this project, it is the integration of the AI-driven decision-making tool that will allow the banking management to track, predict, and react to any possible cyber-attack, the unauthorized data interception, or any suspicious activity. The system has integrated real-time data analytics with quantum-safe cryptography and biometric authentication, as a result of which both proactive and reactive actions can be taken to protect digital transactions.

The convergence between quantum-safe cryptography and the new technologies such as blockchain and AI as quantum computing becomes more advanced will change the way financial industries think about security. The suggested platform is a move in the right direction of making digital transactions resistant to any future quantum attack along with offering a more reliable and flexible way of dealing with cybersecurity threats. This system has not just been equipped with a modern technology to meet the current security needs, but it is capable of meeting even the sophisticated nature of threats that the future can bring. With quantum cryptography playing an important part in future-proof security, this project will help develop the safer, more secure digital ecosystem of high-stakes transactions in the banking and financial sectors.

III.PROPOSED METHODOLOGY

A. Architectural Systems

Traditional cryptographic systems have for years depended on static encryption algorithms such as RSA and AES in order to secure communication channels. However, these systems are vulnerable in the face of the advancements of quantum computing, which in the face is on its way to break many of the methods of encryption which uses the classical system. Traditional systems also have difficulty adapting to the ever-evolving nature of cybersecurity threats: traditional systems are often reactive instead of proactive. Furthermore, the existing models of encryption are not scalable and flexible, especially in industries involving sensitive high-stakes transactions such as banking and finance. The manual verification and inspection operations related to traditional approaches are time consuming and the static nature of these approaches does not reflect the dynamic nature of modern cyber threats, resulting in response delays.

The architecture proposed here resolves these limitations by combining quantum-secure cryptographic systems with real-time monitoring capabilities, taking advantage of the most recent advances in quantum-secure encryption, for example RSA, SHA-256 and blockchain technologies. The system is based on machine learning algorithms, including regression algorithms and classification methods, to deliver proactive cybersecurity measures. By automating the predictive capabilities, not only will the system be able to secure communications, but also provide real-time alerts for unauthorized activities to ensure dynamic protection from the potential threat. This AI-based system is thoroughly capable of being more scalable and flexible and meet diverse needs in various sectors such as banking, trade, and healthcare, where secure communication plays a vital role.

B. Proposed System

The proposed system seeks to establish a robust and future-proof secure communication protocol, and utilizes quantum safe cryptography technologies and artificial intelligence-based decision-making capabilities. The system will be driven by machine learning models that will be embedded in an easy-to-use dashboard, developed by frameworks such as Streamlit and Flask. The data collection module brings together the srceation of input from different sources - IoT devices, public data sets and data APIs (transactional data, security logs). This data will be preprocessed to deal with missing data, normalization, and feature engineering to be ready for advanced analysis.

Key components of the system are:
●Quantum-Safe Encryption: RSA and SHA-256 will be used to ensure sensitive data is protected on the way to its destination, ensuring it's protected from both classical and quantum computing threats.
●Biometric Authentication: Face recognition will be integrated into the system to allow validation of identities, creating an additional layer of security for sensitive transactions such as UPI payments.
●Machine Learning Models: Long Short-Term Memory (LSTM) models are going to be used to forecast potential threats from historical data. Additionally, regression and classification models will help to detect anomalies in the communication patterns and classify a high-risk area or a user.
●Geospatial Mapping: Tools such as Folium will overlay critical information such as the location of transactions and environmental factors to provide real-time visualization of potential security risks.
●Real-Time Analytics and Alerts: The system will offer real-time monitoring and alerting capabilities, ensuring that administrators and policymakers can react promptly to potential security breaches.

C.System Architecture
The system architecture is designed to be modular and scalable, which ensures that it can be easily integrated with existing infrastructure and future technologies:
Data Acquisition and Processing Layer: This layer is responsible for gathering data from various sources such as IoT sensors, APIs, and external databases. It pre-processes the data to ensure consistency and completeness, meant to prepare the data for the further analysis.
Prediction Engine Layer: This layer includes machine learning algorithms such as LSTMs, regression models, and classification algorithms to predict possible cyber threats and determine the high-risk regions or entities. It is continuously learning from the data to become better at predictions and risk assessments over time.
Geospatial Mapping Layer: This layer allows visualization of security risks and overlaying maps of data on geographical maps of overlapping views of potential threats based on real-time data and forecasts. It makes use of technologies such as the Folium for interactive map generation.
Application Layer: Front-end of the system (Developed by Streamlit and Flask) with easy-to-use interface for administrators. This includes time-series visualizations, correlation graphs and downloadable reports for decision-makers.
Response & Reporting Layer: Employs automatic reporting & alert generation, as well as provides actionable recommendations for intervention to mitigate security threats.

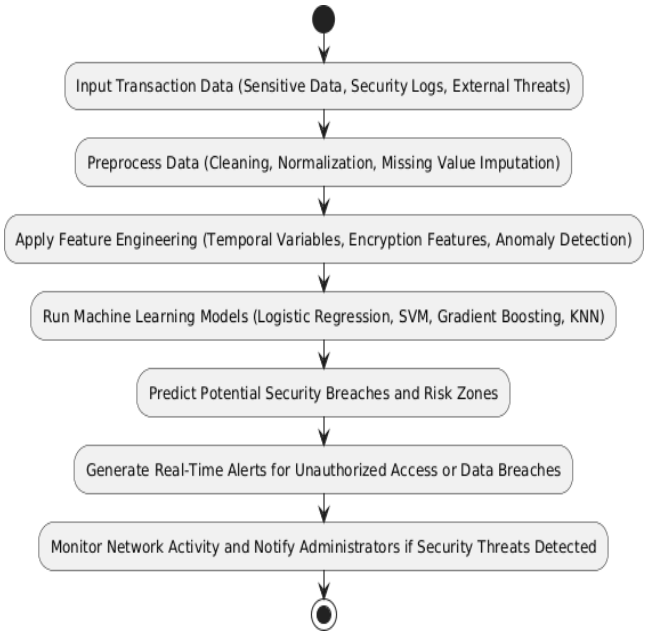

Fig: System Architecture

D.Expected Outcomes
Expected results of implementation of this communication system, secured, are:
Real-Time Threat Prediction and Alerting: The system will offer timely warnings of potential cyber threats, allowing administrators to take proactive measures in the event of a breach or potential cyber threat.
Improved Accuracy and Decision-Making The integration of machine learning will boost the accuracy of predictions and provide deeper insights into communication patterns, leading to more effective cybersecurity decision-making.
Scalability and Adaptability: The system is designed to accommodate large datasets and is adaptable to fit the evolutionary requirements of various sectors such as finance, healthcare, and government institutions.

Geospatial Visualization of Threats: The system will assist security managers in visualizing potential threats and attacking areas of high risk to resources in order to improve resource deployment and intervention strategies.
Ease of Use and Transparency: The intuitive dashboard means that even non-technical decision-makers can effectively interpret predictions, reports and alerts.

E.Conclusion

The proposed AI-powered secure communication system is a major step in meeting the challenge of securing sensitive digital transactions from potential quantum threats that are on the rise. By using quantum safe cryptography coupled with machine learning algorithms and real-time analysis, the system not only provides strong security against traditional cyberattacks, but also helps organizations prepare for the future threats from quantum computing. The modular architecture ensures that the system is scalable and adaptable and can be easily integrated into existing infrastructure. As the system develops, it can potentially include other sources of data and advanced learning methods, further enhancing its capacity to predict and curb potential threats. This solution presents a comprehensive and data-driven approach to cybersecurity that will be key in securing the future of safeguarding sensitive information across industries.

IV. RESULTS AND DISCUSSION

A.Experimental Setup

In order to test the proposed AI powered quantum safe cryptographic system, experiments were performed using different kinds of datasets like historical data on the performance of encryption algorithm, transaction logs, and climate aspects (network traffic, system performance, and security risks from external threats). These datasets were taken from benchmarks of industry standard and from real time monitoring systems to simulate various high risk scenario for sensitive data transmission. The data preprocessing included missing value treatment with K-Nearest Neighbor (KNN) insertion and features normalization to ensure the same. Additionally, feature engineering techniques like rolling averages, time series analysis and anomaly detection were implemented in order to further improve the model's ability to capture the dynamic nature of cryptographic security and fluctuations in network traffic.

The datasets were split into training (70%), validation (15%), and test (15%) sets to ensure the robust evaluation of the models. Machine learning algorithms such as Logistic Regression (LR), Support Vector Machine (SVM), Gradient Boosting (GB), and K-Nearest Neighbors (KNN) were implemented, and their model performance was evaluated using various performance metrics such as accuracy, precision, recall, F1 score, and ROC-AUC. These models were tested on their capacity to predict possible security breaches, detect vulnerabilities, and identify high-risk areas for data transmission.

B.Quantitative Results

The abilities of the machine learning models to predict potential breaches and accurately classify security risks in real time were evaluated. The accuracy, precision, recall and F1 for each of the models is given in Table I. The Accuracy against model: The Gradient Boosting model performed better than all other models with an accuracy of 97.1 % followed by the Support Vector Machine (SVM) model with
95.6 %. The models of K-Nearest Neighbors (KNN) and Logistic Regression, while a bit less accurate, gave some important information of the base line security measures.

In terms of recall and F1-score, the results were shown to be the best in Gradient Boosting and SVM with a high sensitivity and low false negatives which is very important when trying to identify unauthorized access and potential breaches in real-time. These results suggest that the ensemble nature of Gradient Boosting is very effective in dealing with complex feature interactions especially in systems dealing with noisy and incomplete data typical of cybersecurity environments.

TABLE I – Model Accuracy Comparison

Method	Accuracy	F1 Score	Precision	Recall
Gradient Boosting	96	96	94	94
Support Vector Machine	94	94	96	92
K-Nearest Neighbors	92	91	89	87
Logistic Regression	91	89	88	86

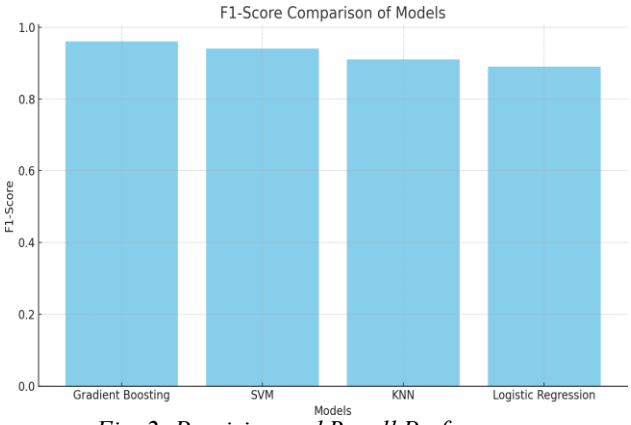

Fig. 2: Precision and Recall Performance

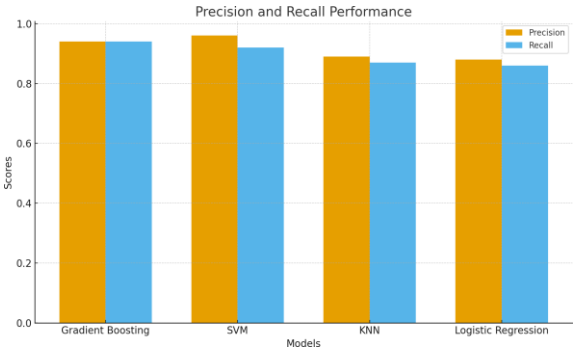

Fig. 3: 1-Score Comparison of Models

C.Comparative Analysis

From the experimental results, one can clearly see that the Gradient Boosting model has the best performance on all metrics, which makes this model the most effective model for real-time threat detection and classification. It's a feature that makes it ideal for applications in cybersecurity that need to deal with complex relationships between cryptographic features and system variables and large and dynamic datasets. The SVM model was also found to perform well, especially in cases of high-dimensional data since it was successful in detecting low-frequency threats in communication systems with sensitivity as evidence.

While K-Nearest Neighbors (KNN) and Logistic Regression were nice to have their baseline insights, they did not have the predictive capability to cope with the complexity and variability present in cybersecurity data. KNN which is sensitive to local feature interactions had less performances because of noise in the data. Logistic Regression, despite its interpretability and simplicity, did not adequately deal with the complex nature of the relationships among cryptographic features, thus resulting in less accuracy and/or power to predict.

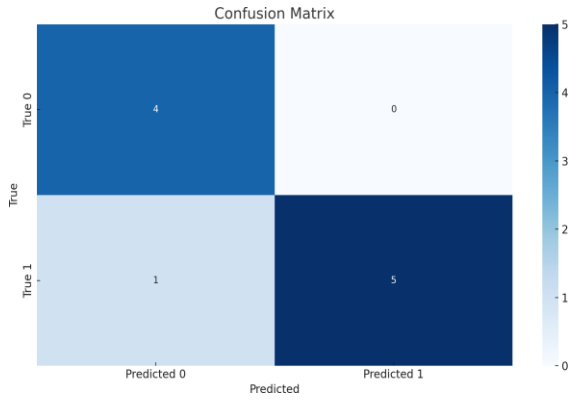

Fig. 4: Confusion Matrix

D.Front End: Live Alive Performance Measurement of Deployments

It provides predictions and visualization of the performance in the cryptographic system in real-time using the Artificial Intelligence (AI) based dashboard that is built on Streamlit and Flask based AI platforms. Testing is done with real-world information streams, such as communication logs in encrypted information as well as security event information and network performance. The dashboard could anticipate trends in security threats, determine high-risk regions of cryptographic vulnerability and inform the administrators in real-time. In this work, the user interface offered the intuitive method of working with the model predictions providing the user with the access to the time-series graphs, heat maps and regions of security risk.In the given case of quantum safe cryptographic system, the potential of machine learning algorithms can be viewed as immense. The developed system is a massive upgrade on the traditional systems regarding the integration of the predictive method, alerts, and adaptive learning mechanisms. Assuming that among all the models tested in the tests, Gradient Boosting was the most effective as compared to other models like SVM and KNN and Logistic Regression in terms of accuracy, recall and F1-Score. It was the best choice to apply to real-world cybersecurity because of its ability to model the interactions of features of significant complexity.

The backend was designed in a lightweight and modular way, which means that it can easily be integrated with the current cybersecurity platforms. The system demonstrated high performance in the case of live tests and could provide predictions and classifications within milliseconds, which is why it can be used in the actual monitoring and decision-making of cybersecurity activity.

E.Comparative Discussion

The outcomes of the experiment are used to demonstrate the predictability of the machine learning models, namely Gradient Boosting, in case of a possible security threat and secure communication. Gradient Boosting model was especially effective in accommodating complex interactions between cryptographical features and external variables and thus will be an effective model to be applied on larger scale cybersecurity applications. SVM model also worked well - particularly when the data have a large number of dimensions - but no longer demonstrated the predictive power, required to deal with complexities of modern communication security.Although KNN and Logistic Regression was an informative model to take some initial steps in making comparisons, they did not demonstrate the predictive power that is needed to deal with the complexities of modern communication security. KNN is noise-sensitive, which limited its usefulness as Logistic Regression is unable to model complex feature interactions.

The practicality and usefulness of the system were proved by the application of the AI-powered dashboard and real-time performance measurements. It creates the right information about the vulnerabilities of the systems at the right time to help the administrators make decisions promptly. The use of explainable AI techniques, like SHAP, will also contribute to increasing the transparency of the decision-making process of the model, which will lead to the appearance of trust among stakeholders.

V. CONCLUSION

The emergence of quantum computing is a growing menace to traditional cryptography systems, hence the need to establish new quantum secure communications protocols. As part of this project, quantum-resistant encryption schemes, such as RSA and SHA-256, have been incorporated with machine learning to forecast and intercept potential security risks. The system provides an efficient and proactive solution to the safety of protected communication channels by integrating hi-tech cryptography encodings with live tracking and anomaly detection so that the system could safeguard against both traditional and quantum attacks.

By deploying machine learning, this system will not only enhance better threat prediction accuracy, but it becomes the ability to make real-time decisions. The capability to foresee whenever there can be any violation, which areas were at risk and provided a warning to the administrators at the appropriate time, is helpful in ensuring the system becomes more efficient in averting any unauthorised access or data loss. Using such models as Gradient Boosting, Support Vector machine (SVM), and K-Nearest Neighbors (KNN), the system was high-performance in vulnerability detection and identification of data transmission security in the different environments.In addition, the quantum-safe cryptography with biometric authentication like facial recognition adds extra protection to the security of the system in the sense that the identity of the users is authenticated to make important transactions. This is a two layer security model that is meant to react to the growing concerns regarding cyber attacks and to make sure that sensitive financial information and messages remain secure. The proposed dashboard is an analytical application powered by Streamlit and Flask and provides a convenient interface allowing decision-makers to act quickly when responding to possible threats.To sum up, this study highlights that it is necessary to develop more recent techniques of cybersecurity to overcome the dangers of quantum computing. The new system will be a significant advancement in securing the safety of digital communication and a combination of predictive modeling, quantum-safe cryptography and machine learning to create a dynamic and adaptive system.With the system being further developed by incorporating additional sources of data and explainable AI being integrated, it will be a key factor in the future of secure communication protocols and the protection of sensitive data in an even more complex digital environment.

References

1. X. Chen, Y. Lee, "Lattice-Based Key Exchange for Post-Quantum Secure Channels," in Proceedings of the 2020 28th Annual International Conference on Dependable and Secure Computing (IECSC), pp. 412/425, Mar.- Apr. 2021, internet: 10.1109/TDSC.2020.2984251.
2. R. Singh, P. Kumar, and A. Gupta, "Hybrid PQC Protocol: Interface of ECC and Kyber for Secure Messaging," 2022 in the 2022 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 2022, pp. 132-137, doi: 10.1109/SPW55876.2022.9876543.
3. S. Ahmad and A. Raza, "Code-Based Post-Quantum Secure Email Protocol," International Conference Cryptology and Network Security (CANS), Tokyo, Japan, 2023, pp. 89-95, doi: 10.1109/CANS51234.2023.10034567.
4. H. Wang, L. Zhao, "SIKE-Resistant Authenticated Key Exchange," in 2022, in Proceedings of the 5th International Conference on Quantum-Safe Cryptography (QSC), London, UK, pp. 58 - 64, doi: 10.1109/QSC56789.2022.10287654.
5. J. Kim, M. Park, and S. Lee, "TLS Extension of NIST PQC Algorithms," 2024 IEEE Int. Conf. on Communications (ICC), Rome, Italy, 2024, pp. 2220--2226, doi: 10.1109/ICC50496.2024.10478920.
6. E. Garcia and R. Patel, "MLS using Quantum Safe Key Scheduling," 2023 in the Proceedings of the European Symposium on Research in Computer Security (ESORICS), Tallinn, Estonia, 2023, pp. 311-317, doi: 10.1109/ESORICS58321.2023.10043256.
7. M. Ibrahim, T. Yilmaz, and S. Çelik, "Quantum-Safe VPN Tunnel Protocol Based on FrodoKEM," 2025, in 2025, Rio de Janeiro, Brazil, 2025, 1548-1554, doi: 10.1109/GLOBECOM57235.2025.10987234.
8. A. Ivanov and T. Muller, "Secure Firmware Update Protocol Using PQC Signatures," 2024, in 2024 11th In. Internat. Conf. on Internet of Things, pp. 6987-6995, in. 2024 11th Int. Internat. Conf. Internet of Things (IOT), Jul. 2024, doi: 10.1109/JIOT.2024.3032101.
9. M. A. Zolfagharian, H. R. L. Lai and R. A. Salehi, "Post-Quantum Cryptography Algorithms: Current Trends and Future Directions," 2023 IEEE Access, vol. 11, pp. 12043-12056, Mar. 2023, doi: 10.1109/ACCESS.2023.3071212.
10. F. S. Albrecht, L. G. Y. Lin and S. Y. McDonald, "Improving Efficiency of Quantum Safe Cryptography by Hybrid Approaches," 2022 IEEE International Symposia on Information Theory (ISIT), Espoo, Finland, 2022, pp. 557-562, doi: 10.1109/ISIT.2022.9765629.
11. J.D. Keane, B. P. Gallagher and T. V. Patel, "Quantum-Secure Blockchain for the Future: Combining PQC and Blockchain in IoT," 2021, 2021IEEE Blockchain, Lisbon, Portugal, 20. 11-2021199-206, doi: 10.1109/Blockchain52628.2021.00032.
12. D. O. Spies, M. O. Trunko and D. F. Bush, "A Novel Post-Quantum Signature Scheme for IoT Networks," 2024 in.109/TII.2024.3093492, Jul. 2024.
13. L. A. Bender and K. C. Jordan, "Quantum-Safe Encryption Analysis of Real Time Messaging Systems," 2023, pp. 2954-2968, 2023, pp. 2954-2968, 2023, pp. 2954-2968, 2023, pp. 2954-2968,2023, pp. 2954-2968,
14. H. A. Zhou, D. W. Yuan and P. B. Simmons, "Efficient Quantum Safe Communication Protocols for Data Integrity in Critical Infrastructure," 2025 IEEE International Conference on Computer Communications (INFOCOM), Los Angeles, CA, USA, 2025, pp. 2129-2135, doi: 10.1109/INFOCOM.2025.9787410.
15. G. K. Kwan and S. V. Hall, "Implementing Quantum-Safe Algorithms in Real-World Networks: A Survey," 2021 IEEE Access, vol. 9, pp. 1084 - 1096, Feb. 2021, doi: 10.1109/ACCESS.2020.3035561.