International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing IoT Communication with the Integration of Quantum Cryptography and Machine Learning

[1]Dr. Adil Ahmed khan, [2]Dr. Pathan Ahmed khan

Submitted:27/01/2024 **Revised**: 05/03/2024 **Accepted**: 12/03/2024

Abstract: The rapid implementation of the Internet of Things (IoT) has raised security concerns, therefore revealing significant vulnerabilities in many sectors, including smart cities, healthcare, and agriculture. This extensive analysis of quantum computing and IoT security devices delineates the advantages of quantum algorithms and the potential for securing communication. Protocols including quantum concepts such as superposition, entanglement, and quantum interference, leading to safe key distribution and authentication procedures, are examined. This paper introduces a novel strategy to reduce the risks that quantum computing presents to IoT systems, which current cryptography solutions fail to adequately address. Quantum computers may use these vulnerabilities to undermine key-pair formation and get private keys from transaction signatures. These transaction signatures are optimized for low-power, cost-effective microcontrollers, such as the ESP32, making the solution accessible for a diverse array of IoT devices. The report features a case study on a post-quantum secure portable device for detecting blood oxygen levels and heart rate, demonstrating the practical advantages and efficacy of the suggested method in improving IoT security against quantum threats. The review addresses quantum key distribution (QKD) protocols, quantum authentication methods proposed as solutions, and the difficulties associated with implementing quantum cryptography techniques in IoT systems. This review assesses the feasibility of quantum-enabled communication, explores its applications across several industries, and examines existing quantum software tools. The objective is to provide a basis for future research and effective practical solutions in the dynamic realm of IoT security.

Keywords: *Iot, Quantum Key Distribution (Qkd) Protocols,* Cryptography, Machine Learning.

Introduction

The Internet of Things (IoT) denotes a network of tangible entities, or "things," equipped with sensors, software, and other technologies. It facilitates their connection and data sharing with other devices and systems over the Internet. The use of IoT is expanding across several applications, including smart grids, urban areas, and intelligent environments. The fast proliferation of IoT applications has resulted in a notable increase in security and privacy concerns, arising from the extensive data produced by these networked devices. Ensuring identification and privacy is essential for IoT apps to properly address the increasing demand while protecting users' security. Quantum computing is crucial for safeguarding the IoT communication network using the principles of quantum physics. It provides robust security measures for IoT components, including data processing, communication, and the management of dynamic data. The primary objective of quantum computing advancement is to build quantum-resistant strategies and processes for addressing IoT security issues. In contrast to quantum computers that use qubits, conventional computers manage discrete bits. These qubits denote the quantum state and the associated probabilities. These qubits serve as a kind of information storage, grounded on principles of quantum physics such as superposition and entanglement. Entanglement generates a robust dependency among quantum particles [4]. The primary advantage of quantum computing is in its capacity to provide secure data and implement intelligent applications for effective decision-making via the use of quantum superposition, quantum property authentication, and quantum key distribution (QKD).In the realm of quantum computing, Quantum Key Distribution (QKD) is a very active research area that enables participants to generate secret keys for secure communication.

Quantum computing can process substantial volumes of data in real-time, potentially laying the foundation for very powerful computing systems. This is particularly pertinent for compute-intensive applications in healthcare, especially within the current fully integrated IoT health IT framework, which encompasses networked medical equipment capable of connecting over the Internet or cloud services [6]. The shift from bits to qubits may greatly enhance pharmacological research in medicine [7]. This research include the examination of protein folding, the assessment of molecular compatibility, including that of pharmaceuticals and enzymes, and the evaluation of the binding affinity among specific biomolecules. Facilitating on-demand computing, redefining medical data security, forecasting chronic diseases, and formulating effective pharmaceuticals. Qubits may facilitate whole-genome sequencing and analysis, enabling faster completion

[1]*System Engineer, Emircom adilkhan403@gmail.com*
[2]*Associate Professor, ISL Engineering College, drpathanahmedkhan@gmail.com*

despite the labor-intensive nature of the procedure [9]. Researchers have examined DNA sequence alignment with Grover's algorithm, doing pairwise alignment via the quantum Fourier transform (QFT). Furthermore, a framework has been established that employs the quantum approximate optimization algorithm (QAOA) to facilitate the reconstruction of de novo DNA sequences. These quantum computing approaches facilitate de novo assembly, an effective method for recreating the original DNA sequence from an unstructured collection of reads, without previous knowledge of the length, organization, or composition of the source DNA. This technique is crucial for analyzing undiscovered species or discovering structural genomic alterations that traditional read mapping tools cannot identify. Furthermore, with the generation of genomic sequences, there has been considerable interest in the analysis of the algorithmic data included within such sequences. A combination of Grover's algorithm and phase estimation has been examined to comprehend the intricacy of the information stored inside these sequences. Quantum computers may facilitate the development of efficient imaging systems that provide enhanced real-time fine-grained clarity for physicians. Furthermore, it may address complex optimization problems associated with formulating the optimal radiation strategy to eradicate malignant cells while minimizing harm to adjacent healthy tissue [10].

Machine learning is the discipline of recognizing patterns in existing data to forecast attributes in fresh data. The model endeavors to discern patterns inside the training data and develops the capability to categorize unknown material as safe or non-secure [2]. However, it is crucial to examine the accuracy and loss throughout the model's training process. Furthermore, it is essential to verify that the model is neither overfitted nor underfitted prior to training, and that the quality and amount of the data are verified by data preprocessing procedures [3]. Upon the model's completion and the assignment of weights according to the training data, achieving minimal validation loss and maximal validation accuracy, the machine learning model is capable of identifying abnormalities in data transfer patterns.

Cryptography has existed since ancient times. It is the practice of transforming a communication into a format that is comprehensible just to the intended receiver. An analogous situation is a letter secured inside a box, accessible just to the receiver who has the key to unlock it. The communication is encrypted and sent to the receiver. In this scenario, if the data is possessed by an intermediary, he or she will be unable to comprehend it [4].

LITERATURE SURVEY

According to Xie et al. [11], Lattice-based encryption serves as a crucial element in the development of future post-quantum cryptography, offering a promising line of defense against potential threats posed by quantum computing. Lattice-based algorithms offer advantages related to speed, efficiency, security, and reduced energy consumption. This work presents a comprehensive analysis and comparison of the most prominent lattice-based cryptosystems. The development and establishment of a dependable post-quantum algorithm continue to be the main challenge in the current exploration of cryptographic solutions for the quantum age.

Broadbent et al [12], advocated the establishment of the principles of QKD, followed by an exploration of the development of QKD networks and their actual applications. The overall structure of the QKD network, including its components, interfaces, and protocols, is then delineated. The relevant physical layer and network layer solutions are comprehensively detailed, followed by an examination of standardization activities and quantum key distribution network application scenarios. Ultimately, it explores prospective directions for future research and presents design concepts for quantum key distribution networks.

Yuan et al. [13], Examine contemporary research subjects include quantum computing, quantum walks, cryptography, big data, autonomous vehicles, image processing, artificial intelligence, fuzzy logic, cooperative systems, swarm optimization, and security. They used a distinctive search methodology to gather data from the Dimensions database, highlighting that the results are limited to published works on quantum computing-based IoT security. Subsequent study will use a broader array of data sources.

Aslam et al. [14] unveiled a novel quantum-classical neural network, Res-QCNN, based on deep latent training. The training methodology for evaluating IoT systems consists of a residual structural block integrated with a quantum neural network. The research examines the merits and drawbacks of integrating quantum concepts with deep residual learning. Res-QCNN surpasses previous models in learning a unitary function and demonstrates robustness to noisy input.

Ygalet al. [15] contributed modifications to PHOTON-Beetle, Ascon, Xoodyak, and Sparkle, four lightweight hash functions that advanced to the National Institute of Standards and Technology's (NIST) final stage of the standard competition. These enhancements produced remarkable hashing throughput on a GPU platform, ranging from 70 Gbps to 1000 Gbps, which made them perfect for high-performance data integrity checks in

Internet of Things applications. The effectiveness of these hashing algorithms on a quantum computer was also assessed by the research using ProjectQ.

Vuiket al. [16] championed a comprehensive analysis of the ramifications of quantum computing on the security of 5G mobile communications. This research results in a sequence of clear, gradual improvements aimed at ensuring the security of 5G, along with 3G and 4G. They presented a multi-phase method to enhance security and ensure a seamless transition to a post-quantum-secure system by using the backward compatibility characteristics inherent in the 5G security architecture.

Bansaletal[17] Proposed recommendations for the next generation of IoT developers on constructing quantum-resistant systems. The notion of quantum encryption is novel in the domain of cryptography. In comparison to traditional encryption, its primary benefits are the identification of sniffers and absolute security. Enhanced quantum cryptography has been developed for private-sector enterprises such as banking. The time for quantum cryptography techniques is now, as the Internet of Things has subjected billions to the threat of personal information, device data, and the advancement of quantum computing.

Yanget al [18] Proposed to address a binary optimization problem with Quantum Annealing (QA) inside an IoT network to get the optimal scheduling approach. Real-time solutions may be achieved by defining certain challenges according to specified design requirements. QA surpasses its competition regarding computing efficiency. Nonetheless, there exists an embedding process that, in the case of substantial problems, may postpone convergence at the designated period.

IOT SECURITY THREATS

Innovative applications like as smart cities, agriculture, and healthcare have expedited the development of IoT-enabled communication. These IoT devices produce substantial quantities of data in various situations. With the proliferation of IoT applications, the possibility of attacks that jeopardize user privacy concurrently increases. Authentication, integrity, authorization, and trust management are critical security concerns in an Internet of Things ecosystem.Figure 1 illustrates the main security problems inside the IoT layered architecture. This section examines the benefits of using a quantum layer to enhance IoT security and addresses issues within the IoT architecture.

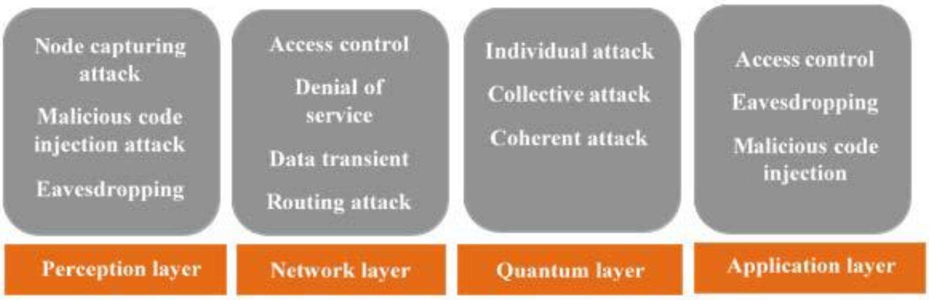

Fig.1. Security threats on IoT layer architecture

Figure 1 illustrates the architecture of the IoT layer. This reveals several security weaknesses at various tiers. The perception layer, responsible for gathering ambient data via sensors, faces threats such as sensor node compromise, data falsification, and eavesdropping. Unrestricted internet connection renders the network layer vulnerable to access control attacks, denial of service threats, and data interception. The incorporation of a quantum layer improves IoT security via secure key distribution; yet, it simultaneously adds new vulnerabilities, since quantum cryptography may be susceptible to individual, collective, and coordinated attacks. The application layer, which provides services for user decision-making, faces several challenges, including eavesdropping, access control breaches, service interruptions, and the infiltration of malicious code.

A. Quantum Fundamentals

The design of traditional computers considers the impact of noise on transistor performance, especially when transistors decrease in size. Consequently, their circuits are designed to mitigate the impact of quantum events. Conversely, quantum computers use a distinct approach by using quantum bits (qubits) rather than conventional bits. These qubits exhibit two quantum states, analogous to classical bits denoting 0 or 1, however they also have distinctive quantum characteristics. They may exist in a superposition, concurrently representing values 0 and 1, resulting in the intriguing notion of superposed bits. The three traits are enumerated as follows [21]. Superposition: Superposition is a fundamental property of quantum mechanics that permits the amalgamation of two quantum states to generate an additional legitimate quantum state. This concept enables a quantum system, such as a quantum particle or qubit, to concurrently exist in different locations or states. It enhances quantum computing via very high-speed parallel processing, markedly differentiating it from conventional systems constrained by binary restrictions. In the realm of quantum computing, information may exist in two states simultaneously, revealing extraordinary computational potential.

Entanglement: Entanglement is the phenomena whereby a pair or group of particles interact so that the quantum state of each particle cannot be independently stated; rather, it must be considered in relation to the states of the other particles in the system. This extraordinary property of entanglement endures even when the particles are physically separated by considerable lengths.

Interference: In quantum computers, interference serves a role analogous to wave interference in conventional physics. Two waves interacting inside the same medium are described as interfering with each other. When waves align in the same direction, they produce a resultant wave termed constructive interference; conversely, when waves align in opposing directions, they provide a resultant wave.

MACHINE LEARNING AND CRYPTOGRAPHY BASED AUTHENTICATION APPROACH

A. Behaviour based Biometric Authentication

Behavior-based biometrics may be used to monitor distinct human behavior patterns, such as typing speed and mouse click patterns, among others [6]. This kind of profile may be created via machine learning approaches through the constant observation of user behavior patterns. A zero-knowledge proof may be derived from this behavioral biometric user profile, which serves as a mathematical representation of the person's behavioral biometrics. A mix of biometric behavioral traits is exclusive to each person, making replicas very improbable. The behavioral biometric profile of each user is affixed to the cryptographic token in a zero-knowledge proof manner. To decrypt the data, a user must first provide their behavioral biometric profile, which is transformed into a zero-knowledge proof and compared with the saved token. Subsequently, the decryption key is requested to facilitate the data decryption. This method is more secure than a conventional cryptography-based security strategy, since it provides an additional layer of protection for the data in use.

B. Anomaly Detection for Data Transfer

Machine learning techniques may identify underlying irregularities in data transmission procedures [7]. The data is transformed into ciphertext by homomorphic encryption. The encrypted data is thereafter sent via various routes to many recipients. Advanced machine learning methodologies are used on encrypted data for the purpose of anomaly detection. These algorithms can ascertain if the data on the receiving end has been compromised. If the data seems to be compromised, it will be deleted, and the original data will be reencrypted. Decrypting the data is unnecessary, since machine learning algorithms can identify abnormalities in both encrypted and decrypted formats.

C. Voice Biometrics with Lattice Based Cryptography

The voices of authorized users are captured and transformed into a mathematical template. The transformed mathematical template is then encrypted using lattice-based encryption and sent across the channel alongside the encrypted data. Lattice-based encryption is very secure and remains impervious to decryption, even with quantum computer capabilities. The data is secured using traditional cryptographic techniques such as RSA or ECDSA. The encrypted data and the encrypted speech template are sent to the recipient. At the receiver's end, the voices of authorized users are captured and then transformed into a mathematical template. The transformed mathematical template is then encrypted using a lattice-based cryptographic technique. If the encrypted speech templates of both the sender and recipient match, users are allowed and granted access to the data.

D. Quantum Key Distribution

Quantum Key Distribution (QKD) is a novel method used to produce a highly secure encryption key that is shared between the sender and the recipient. Quantum Key Distribution (QKD) employs the principles of quantum physics and exploits photons, the fundamental particles of light, to generate the cryptographic key. These photons often incorporate quantum information, including polarization states, inside their encoding. If someone attempts to intercept the encrypted data during transmission, it will trigger an alarm to both the sender and recipient, indicating a possible security violation. Comprehensive data transfer security is attained by the use of a shared key for encryption, which encodes data at the sender's end and decodes it at the receiver's end after authentication and validation.

This quantum-resistant technology provides robust protection against both future quantum and conventional threats, establishing it as an innovative solution for secure data transmission.

E. NTRUEncrypt

The strength of NTRUEncrypt relies on the challenges posed by lattice difficulties, particularly the Ring-LWE problem [9]. It is resilient to both traditional and quantum cyber threats. The data designated for transmission is converted into a vector and then multiplied by the public key, represented as a lattice.

The private keys are vectors included inside this lattice. Additionally, an error component is used during transmission to create a degree of randomization. The original data may be recovered by using the private key to identify the shortest vector inside the lattice that approximates the encrypted vector as closely as feasible. This is a quantum-safe methodology, since it constitutes an NP-hard issue; finding the shortest vector inside a randomized lattice presents a formidable mathematical challenge.

F. Code Based Cryptography

This cryptography relies on error correcting codes. The data designated for transfer is compromised due to an error. The construction of the private and public key is derived from error correcting code [10]. The generation of the private key utilizes an irreducible Goppa code, while the public key is formed using a random generator matrix derived from the variations in Goppa Code. The data, upon arrival at the receiver, can solely be decrypted by individuals possessing the private key. This technique aims to minimize the dimensions of encryption and decryption keys. This cryptography technique demonstrates a high level of security and exhibits resistance to quantum threats. Quantum computers possess the capability to tackle numerous complex mathematical problems, forming the foundation for various cryptographic techniques. Cryptography that relies on code is fundamentally grounded in a range of mathematical principles, which are crucial in the context of potential quantum threats.

IOT ENABLED BY QUANTUM TECHNOLOGY

The Internet of Things (IoT) framework interlinks diverse heterogeneous devices using many wireless protocols, such as WiFi, Bluetooth, Zigbee, and 6LOWPAN, which are essential enabling technologies for IoT. These advancements enhance data transmission for applications like precision agriculture, sophisticated healthcare systems, and intelligent urban environments. The amalgamation of IoT with quantum computing is essential for these applications, since they need data privacy and secrecy. Although conventional cryptography, including public and private key methods, presently safeguards IoT communications, quantum computers are anticipated to compromise this security. Theoretically, the public-key infrastructure is already threatened by quantum algorithms such as Shor's and Grover's. If these security concerns are not resolved, eavesdroppers may exploit vulnerabilities via teleportation-based attacks, man-in-the-middle attacks, and denial-of-service assaults [31]. Identified risks include pulse-energy monitoring, laser damage, laser seeding, information leakage (via Trojan horses), source faults, side-channel assaults, device calibration discrepancies, and timing attacks. Quantum cryptography provides a formidable alternative for secure communication, addressing these dangers and connecting theoretical concepts with practical implementation [32]. Due to the resource limitations of IoT devices, safeguarding sensitive data necessitates lightweight encryption that aligns with their restricted processing capacities [33]. Furthermore, with the rise of both classical and prospective quantum assaults, the implementation of quantum-resistant encryption is essential. Lattice-based encryption has potential as a safe and efficient method for post-quantum cryptography [34]. The evolution of IoT connectivity necessitates the integration of quantum computing to provide safe and robust communication routes.

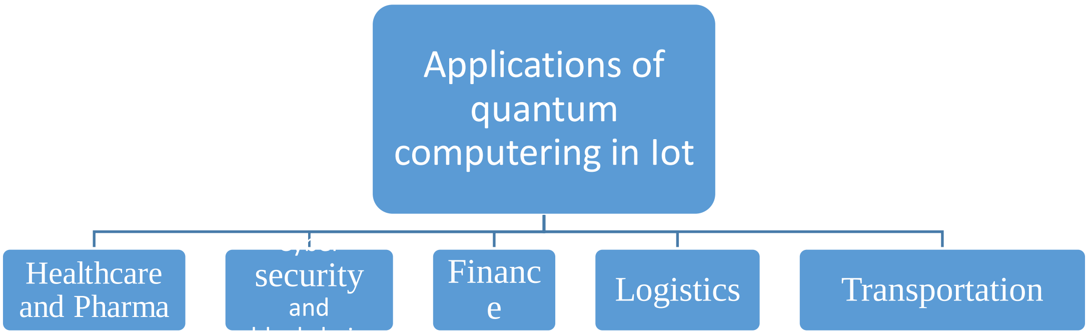

Fig.3. Applications of quantum computing in IoT [3]

Figure 3 illustrates the many uses of quantum computing in the Internet of Things, emphasizing its capacity to address a wide range of difficulties across different sectors. Quantum computers may address challenges in the banking sector, including financial chores, and have also been used in the healthcare and pharmaceutical fields, especially in drug development. Quantum computing can enhance blockchain solutions for addressing supply chain challenges in logistics and facilitate encrypted transactions for superior cybersecurity. Quantum computing may also assist in wave propagation systems and traffic management.

Healthcare and Pharma: Drug research is costly because molecular simulations need a lot of computational resources. Research and development in the pharmaceutical industry may benefit from the usage of quantum computers due to their ability to accurately reproduce quantum phenomena. Biogen and Accenture worked together on quantum computing applications for drug development. Another sector that has benefited from quantum computing is healthcare.Staying on top of one's lifestyle is crucial for managing chronic conditions.

Cyber security and blockc hain: Because it relies on cryptographic methods, blockchain is susceptible to sophisticated assaults; yet, it is used for encrypted transactions and contracts. One way to prepare for future problems is to look at quantum blockchain. Even while Accenture has recognized the blockchain's potential relationship with quantum computing, post-quantum cryptography—algorithms that can resist the attack of Microsoft's and Google's strong quantum computers—is gaining popularity. More and more, cyber security companies are focusing on this sector. Quantum computers may one day solve all of the banking industry's problems, including market prediction, fraud detection, risk analysis, asset pricing, and portfolio optimization. Logistics: Quantum computing shows promise since traditional computers struggle to handle complicated supply-chain problems. Because of its importance in route optimization, the traveling salesman problem—in all its variants—presents a formidable obstacle for NISQ devices in the transportation sector. Whether you're dealing with autonomous or conventional cars, the optimization problems you face when managing a big fleet are always evolving. The most effective demonstration of quantum computing is the traffic optimization project that Volkswagen is collaborating on with D-Wave [35].

PROCESS FLOWCHART

Figure 2 illustrates the whole process flowchart demonstrating the execution of a secure data transmission system via the strategic integration of cryptographic methods and Machine Learning (ML) algorithms. The flowchart has eight primary steps: Data Transfer Initiation, Data Encryption, Data Transfer, Machine Learning Authentication, Data Decryption, Data Processing and Validation, ML-Based Anomaly Detection, and Final Verdict. A sender initiates the data transmission. Subsequently, data is encrypted using several cryptographic methods such as RSA, AES, and NTRUEncrypt. In asymmetric encryption, a key pair is formed consisting of a public key and a private key for the purposes of data encryption and decryption. The public key may be disseminated to anybody, while the private key is safeguarded by the owner. The sender employs the recipient's public key to encrypt the data, while the recipient utilizes the sender's private key to decode it. The encrypted data is sent over a secure data transfer protocol across a protected channel to the designated recipient. Prior to the receiver receiving the data, user authentication is verified by machine learning algorithms. The machine learning algorithms evaluate user behavioral data such as keystrokes, mouse movements, face recognition, and speech to determine user authorization. The authorized user is able to decode the communication with a decryption algorithm. Typically, identical techniques for decryption and encryption are used in the process. The recipient then processes the data and verifies its integrity. Upon verification of data veracity, abnormalities are identified using machine learning algorithms. Anomalies are identified by the analysis of user behavior or the surveillance of system hazards. Should the sent data exhibit abnormalities, the system will generate an alert and refuse the data transfer. If no discrepancies are identified in the data, it will be used for further purposes.

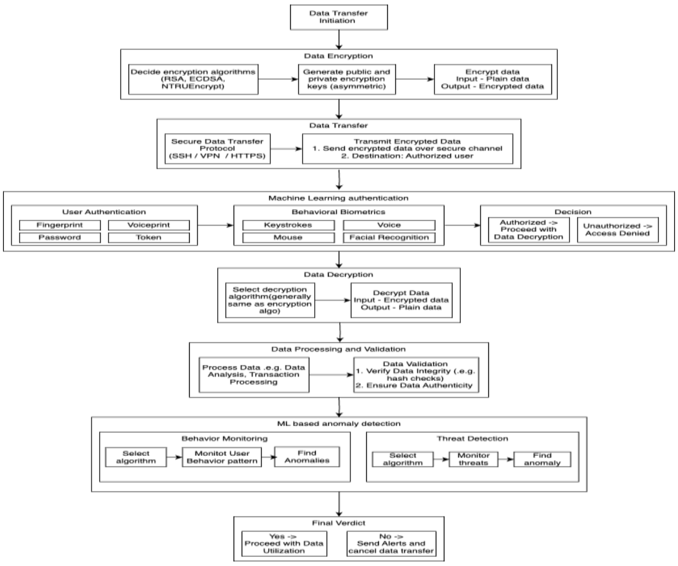
Data Transfer Initiation
Data Encryption
Decide encryption algorithms (RSA, ECDSA, NTRUEncrypt)
Generate public and private encryption keys (asymmetric)
Encrypt data Input - Plain data Output - Encrypted data
Data Transfer
Secure Data Transfer Protocol (SSH / VPN / HTTPS)
Transmit Encrypted Data 1. Send encrypted data over secure channel 2. Destination: Authorized user
Machine Learning authentication
User Authentication
Fingerprint
Voiceprint
Password
Token
Behavioral Biometrics
Keystrokes
Voice
Mouse
Facial Recognition
Decision
Authorized -> Proceed with Data Decryption
Unauthorized -> Access Denied
Data Decryption
Select decryption algorithm(generally same as encryption algo)
Decrypt Data Input - Encrypted data Output - Plain data
Data Processing and Validation
Process Data .e.g. Data Analysis, Transaction Processing
Data Validation 1. Verify Data Integrity (.e.g. hash checks) 2. Ensure Data Authenticity
ML based anomaly detection
Behavior Monitoring
Select algorithm
Monitot User Behavior pattern
Find Anomalies
Threat Detection
Select algorithm
Monitor threats
Find anomaly
Final Verdict
Yes -> Proceed with Data Utilization
No -> Send Alerts and cancel data transfer

Fig. 1 Flowchart showing the detailed implementation process of a secure data transfer system using ML and cryptography [2]

Conclusion

The Internet of Things (IoT) offers users a plethora of advantages that assist them in making well-informed choices. These benefits are made possible by the Internet of Things' ability to link various devices. On the other hand, owing to the sensitive nature of the data that these apps manage, particularly in the settings of the military, smart cities, and healthcare, stringent security measures are essential. Traditional encryption methods are becoming more vulnerable to assaults from quantum computing due to the fact that they are dependent on complex mathematical concepts. For this reason, it is very necessary to implement quantum-based security in order to safeguard Internet of Things communications against the possibility of quantum attacks. This analysis provides a comprehensive overview of the security threats that are associated with applications that are connected to the Internet of Things. In addition to investigating quantum-resistant security solutions, quantum authentication schemes, and quantum key distribution (QKD), this research addresses these issues. In addition to this, it highlights the necessity of quantum-based encryption approaches for ensuring secure communication between Internet of Things devices and addresses the challenges that arise when attempting to integrate quantum capabilities into Internet of Things systems.

An essential development that will have profound repercussions across a broad variety of businesses, including educational institutions, high-frequency trading, and many others, is the strategic combination of machine learning methods with cryptography techniques for the purpose of enabling the secure transfer of information. The confluence of these breakthroughs brings the security of data to new heights, spanning a wide variety of safeguards, covering a wide spectrum of potential threats. via the use of the unassailable fortress of data encryption, multi-layered user authentication, novel security approaches, and machine learning-driven detection of abnormalities, businesses are able to guarantee the confidentiality of private data during its intricate journey via networks and data storage facilities.

References:

[1] Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero and M. Polsinelli, "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2024.3485796.

[2] Dr. B. Sathananth, J. Selvin Jeba Singh, Exploring The Intersection Of Quantum Computing And Internet Of Things Security: A Comprehensive Survey, Issn (Print): 2393-8374, (Online): 2394-0697, Volume-6, Issue-7, 2019.

[3] Aryyama Kumar Jana1, Srija Saha, Integrating Machine Learning with Cryptography to Ensure Dynamic Data Security and Integrity, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 , Volume 11 Issue X Oct 2023- Available at www.ijraset.com

[4] Udoh, I.S. and Kotonya, G. (2018), Developing IoT applications: challenges and frameworks. IET Cyber-Physical Systems: Theory & Applications, 3: 65-72. https://doi.org/10.1049/iet-cps.2017.0068.

[5] Sun, Li, and Qinghe Du. 2018. "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions" Entropy 20, no. 10: 730. https://doi.org/10.3390/e20100730.

[6] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy and A. Ghoneim, "Secure Quantum Steganography Protocol for Fog Cloud Internet of Things," in IEEE Access, vol. 6, pp. 10332-10340, 2018, doi: 10.1109/ACCESS.2018.2799879.

[7] Usenko, Vladyslav C., and Radim Filip. 2016. "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense" Entropy 18, no. 1: 20. https://doi.org/10.3390/e18010020.

[8] Alshammari, Majid R., and Khaled M. Elleithy. 2018. "Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks" Sensors 18, no. 10: 3569. https://doi.org/10.3390/s18103569.

[9] Thomford, Nicholas Ekow, Dimakatso Alice Senthebane, Arielle Rowe, Daniella Munro, Palesa Seele, Alfred Maroyi, and Kevin Dzobo. 2018. "Natural Products for Drug Discovery in the 21st Century: Innovations for Novel Drug Discovery" International Journal of Molecular Sciences 19, no. 6: 1578. https://doi.org/10.3390/ijms19061578.

[10] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018, doi: 0.1109/ACCESS.2018.2817615.

[11] Xie, J., Hu, Yp., Gao, Jt. et al. Efficient identity-based signature over NTRU lattice. Frontiers Inf Technol Electronic Eng 17, 135–142 (2016). https://doi.org/10.1631/FITEE.1500197.

[12] Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. Des. Codes Cryptogr. 78, 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4.

[13] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information

Fusion," in IEEE Access, vol. 6, pp. 23626-23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

[14] A. Aslam and E. Curry, "Towards a Generalized Approach for Deep Neural Network Based Event Processing for the Internet of Multimedia Things," in IEEE Access, vol. 6, pp. 25573-25587, 2018, doi: 10.1109/ACCESS.2018.2823590.

[15] Bendavid, Ygal, Nasour Bagheri, Masoumeh Safkhani, and Samad Rostampour. 2018. "IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function" https://doi.org/10.3390/s18124444. Sensors 18, no. 12: 4444.

[16] Möller, M., Vuik, C. On the impact of quantum computing technology on future developments in high-performance scientific computing. Ethics Inf Technol 19, 253–269 (2017). https://doi.org/10.1007/s10676-017-9438-0.

[17] I. Bhardwaj, A. Kumar and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2017, pp. 504-509, doi: 10.1109/ISPCC.2017.8269731.

[18] Q. Yang and S. -J. Yoo, "Optimal UAV Path Planning: Sensing Data Acquisition Over IoT Sensor Networks Using Multi-Objective Bio-Inspired Algorithms," in IEEE Access, vol. 6, pp. 13671-13684, 2018, doi: 10.1109/ACCESS.2018.2812896.

[19] Ruan, Y., Chen, H., Tan, J. et al. Quantum computation for large-scale image classification. Quantum Inf Process 15, 4049–4069 (2016). https://doi.org/10.1007/s11128-016-1391-z.

[20] Vermaas, P.E. The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable. Ethics Inf Technol 19, 241–246 (2017). https://doi.org/10.1007/s10676-017-9429-1.

[21] Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. Des. Codes Cryptogr. 78, 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4.

[22] Usenko, Vladyslav C., and Radim Filip. 2016. "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense" https://doi.org/10.3390/e18010020.Entropy 18, no. 1: 20.