Networks and Heterogeneous Media

NHM, 18(3): 1313–1334.
DOI: 10.3934/nhm.2023057
Received: 30 January 2023
Revised: 06 April 2023
Accepted: 10 April 2023
Published: 5 May 2023

https://aimspress.com/journal/nhm

Research article

Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology

Santosh Kumar Henge[1], Gitanjali Jayaraman[2], M Sreedevi[3], R Rajakumar[3], Mamoon Rashid[4,*], Sultan S. Alshamrani[5], Mrim M. Alnfiai[5] and Ahmed Saeed AlGhamdi[6]

[1] Department of Computer Applications, Directorate of Online Education, Manipal University Jaipur, Rajasthan, India
[2] Department of Information Technology, Vellore Institute of Technology, 632014, Vellore, India
[3] Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, 517325 Madanapalle, India
[4] Department of Computer Engineering, Faculty of Science and Technology, Vishwakarma University, Pune, 411048, India
[5] Department of Information Technology, College of Computers and Information Technology, Taif University, Taif PO Box 11099, Taif, 21944, Saudi Arabia
[6] Department of Computer Engineering, College of Computer and Information Technology, Taif University, PO Box. 11099, Taif 21994, Saudi Arabia

* **Correspondence:** Email: mamoon873@gmail.com.

Abstract: The central remote servers are essential for storing and processing data for cloud computing evaluation. However, traditional systems need to improve their ability to provide technical data security solutions. Many data security challenges and complexities await technical solutions in today's fast-growing technology. These complexities will not be resolved by combining all secure encryption techniques. Quantum computing efficiently evolves composite algorithms, allowing for natural advances in cyber security, forensics, artificial intelligence, and machine learning-based complex systems. It also demonstrates solutions to many challenging problems in cloud computing security. This study proposes a user-storage-transit-server authentication process model based on secure keys data distribution and mathematical post-quantum cryptography methodology. The post-quantum cryptography mathematical algorithm is used in this study to involve the quantum computing-based

distribution of security keys. It provides security scenarios and technical options for securing data in transit, storage, user, and server modes. Post-quantum cryptography has defined and included the mathematical algorithm in generating the distributed security key and the data in transit, on-storage, and on-editing. It has involved reversible computations on many different numbers by super positioning the qubits to provide quantum services and other product-based cloud-online access used to process the end-user's artificial intelligence-based hardware service components. This study will help researchers and industry experts prepare specific scenarios for synchronizing data with medicine, finance, engineering, and banking cloud servers. The proposed methodology is implemented with single-tenant, multi-tenant, and cloud-tenant-level servers and a database server. This model is designed for four enterprises with 245 users, and it employs integration parity rules that are implemented using salting techniques. The experimental scenario considers the plain text size ranging from 24 to 8248 for analyzing secure key data distribution, key generation, encryption, and decryption time variations. The key generation and encryption time variations are 2.3233 ms to 8.7277 ms at quantum-level 1 and 0.0355 ms to 1.8491 ms at quantum-level 2. The key generation and decryption time variations are 2.1533 ms to 19.4799 ms at quantum-level 1 and 0.0525 ms to 3.3513 ms at quantum-level 2.

Keywords: secure keys; quantum cryptography; artificial intelligence; homomorphic cryptosystem; public key; quantum digital signature

1. Introduction

Cloud computing is a centralized server-based distributed data processing, security, and storage environment. Cloud computing is becoming increasingly important in our technologically dependable daily lives. The obvious challenge is to create a globalized computing environment while maintaining end-user data security and privacy. A digital system is primarily thought to be a resourceful collective computation machine that is intelligent enough to impersonate any physical computation machine while increasing calculation time by, at most, a polynomial factor. It may not be confirmed when quantum mechanics is considered [1]. One of the complexes weakening the necessary implication processing in the constant-variable quantum digital signature (QDS)-based protocol [2] is the side-channel attack (SCA).

In today's fast-paced technological world, traditional computers are limited in addressing future data security complexities. Even if all humanity's computations can solve data security problems but fail to provide satisfactory results, in this case, quantum computers (QC) show many technical solutions for data leakage in data processing [3]. With the help of classical computational techniques implicated in safe data-processing tasks, QC plays a significant role in potentially secure data processing [4]. The QC can operate on qubits with superposition of quantum states functionality. The qubits are involved with 0 or 1, 0 and 1, or a simultaneous permutation of 0 and 1. The QC encodes information with qubits using various quantum conditions, such as 0 or 1, 0 and 1, or a simultaneous overlay of singular figures. It isn't easy to invert the encryption stage levels if only public key (PuK) cryptosystems (CSs) are available. The Shor's are active algorithmic sequences for factoring operations on CSs that are broken if a short algorithmic series aims to resolve the distinct logarithmic problematic statements. Quantum computer applications are used to break cryptographic codes in real-time experimental scenarios. As illustrated in Figure 1, quantum procedures aid in achieving subtler

cryptographic goals and the required distribution. QC implies using fine quantum mechanical properties such as the Heisenberg uncertainty principle and the quantum no-cloning theorem [5] to make performing quantum cryptography (QuCr) related operations unbearable by using conventional-based cryptography sequences.

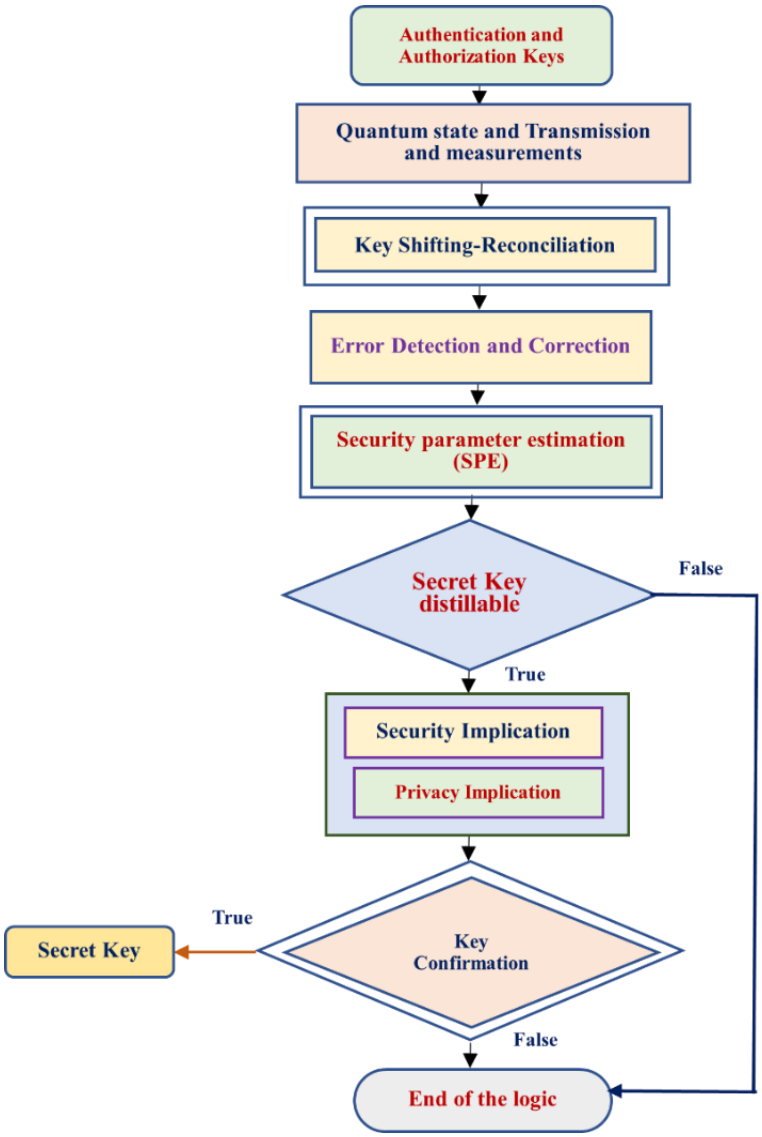

Figure 1. Quantum key distribution protocol execution stages.

Quantum computing efficiently processes the composite algorithms, allowing for innovative advances in cyber security, forensics, artificial intelligence, and machine learning-based complex systems. It also demonstrates solutions to many challenging problems in cloud computing security.

- This study proposes using quantum computing to distribute security keys using the post-quantum cryptography mathematical algorithm. It recommends security scenarios with technical feasibility for securing data in transit, storage, user, and server modes.
- Post-quantum cryptography has framed and implicated the mathematical algorithm in generating the distributed secure key and the data in transit, storage, and editing modes.

- By superpositioning the qubits for providing quantum services and other product-based cloud-online access, it has implicated reversible computations on many different numbers. It also processes artificial intelligence-based hardware service components for end users.

The QC methodology algorithmic sequences demonstrate accurate and sophisticated solutions to the problems that industries and enterprises face. To overcome many unsolvable security threads, artificial intelligence (AI), machine learning (ML), and deep learning (DL)-based systems and models will be integrated with QC. These blended, hybrid computational approaches will be required to build self-auto-tuning intelligent systems to provide efficient security and privacy for every data mode. We identified established obstacles as the greatest and administrative obstacles as the second level of the most significant international substance classification between the leading QC questions challenging the banking, financial, software, defence, and stock market industries by integrating QC with AI, ML, and DL. This study will help researchers and industry experts prepare specific scenarios for synchronizing data with medicine, finance, engineering, and banking cloud servers. The proposed methodology is implemented with single-tenant, multi-tenant, and cloud-tenant-level servers and database servers. This model is designed for four enterprises with 245 users, and it employs integration parity rules that are implemented using salting techniques. In the experimental scenario, consider the plain text size ranging from 24 to 8248 for analyzing secure keys, data distribution key generation, encryption, and decryption time variations. The key generation encryption time variations are 2.3233 ms to 8.7277ms at quantum-level 1 and 0.0355 ms to 1.8491 ms at quantum-level 2. The key generation encryption time variations are 2.1533 ms to 19.4799 ms at quantum-level 1 and 0.0525 ms to 3.3513 ms at quantum-level 2.

This next section of the article is structured as follows: Section 2 includes the relevant literature content as well as the research context; Section 3 contains the proposed approach, which is based on secure keys data distribution in the user-storage-transit-server authentication process using mathematical post-quantum cryptography methodology with Quantum-based Secret Sharing (QbSS), Post-Quantum Cryptography (PQC) implications with four phases of execution along with Qu. The experimental analysis is presented in Section 4; the results and discussion are presented in Section 5; and the conclusions and future directions are presented in Section 6.

2. Related work

This section provides insight into various quantum computing-based cryptography (QCbC) approaches and advances in traditional cryptography techniques [6]. The different study states that the QCbC used the controlled properties of QC techniques like QC-No-Cloning-Assumption (QC-NCA) and QC-Heisenberg-Vagueness-Rule (QC-HVR) [7] to enrich the standard cryptography techniques.

Generally, conventional cryptography (CC) has implicated security scenarios with the unverified computational hypothesis. The QCbC has proposed some secure applications with the technical implications of quantum-based key distribution (QbKD) and high success rates. The QbKD provides unconditional security scenarios for securing data in transit, storage, user, and server modes. The experimental performance of QbKD has been improved and successfully implemented over hundreds of kilometres over both good, industry-standard telecommunication fibre optical and wire-less communication channels. Profitable QbKD environments are presently accessible in many enterprises, like telecom companies and industries [8]. The universal quantum integrated systems harmony to solve convinced mathematical complications in a well-organized way compared to their classical base-level counterparts. I. S. Kabanov et al. have integrated innovative analysis to push new limits in information

security in communications, distributed data, and cloud storage applications using conventional, traditional, hybrid, traditional-conventional-quantum, and PQC environments. This research analyzed recent critical characteristics, state-of-the-art, advanced inclinations, and the restrictions of these practices for enterprise-level data security appliances [9].

The author D. A. Kronberg investigated the innovative nature of the outbreak using intelligible QKDP. It involves measurement exclusively at the interrupted state levels by sending the rest unaffected; it also integrates the optimum value computations, which are considered attack constraints for a random distance mode of data passing channels. This analytical research compared this innovative attack with typical splitting beam attacks [10]. In another study, the quantum computer's (QC) operations and computations were measured based on Shor's algorithmic statements to provide super-quick solutions to various mathematical problems [11]. QKD is a quantum-based key-proof replacement structure treated as influential by the imminent data transformation industries. The vital module in QKD is the data resolution step used to alter the quantum channel's noisy faults. The authors, E. O. Kiktenko et al., recommended the development of a protocol that integrates the data reunion. It endorses essential growth in the competence of the practices and plummets its internal actions; the projected techniques present symmetries concerning involved parties' operational consequences along with deliberation of outcomes of ineffective belief-propagation decoding scenarios [12].

Bruno Huttner et al. described the goals of the Quantum-safe security group, which are used to provision the quantum-safe cryptography communities in deployment and development. They proposed a framework to shield data during rest or movement [13]. The author, Kartik Hirapara, has presented the importance of QC and stated that it is a basket of current security protocols that protect worldwide financial markets and government organizations [14].

The author in [15] described the coordination relationship between QC and Shor's algorithmic sequences (SAS), which smartly use the possessions of quantum parallelism (QP). QP generates the prime factorization problem's best outcome consequences in less computation time. In addition, the author also suggested that it is possible to yield the best results by integrating QC techniques with the leverage of artificially intelligent systems, learning approaches, cloud computational architectures, and large-data models. It helps to accelerate QC development. Peter W. Shor has proposed the quantum computing factoring of integers used to generate discrete logarithmic sequences; it is mainly presumed to be inflexible on conventional systems and has been implicated based on numerous projected CSs. The sharp randomized logarithmic lines are specified for two complications based on a theoretical QC. The supporting phases are multinomial in input size: quantity of numerals to be factored [16].

The authors Bernstein. D. J. et al. have described the various shields used to securely store and communicate information to avoid attackers from data leakage [17]. The author, Shi-Hai Sun et al., have proposed the approach of hacking on a decoy-state QKD scheme with the fractional stage of randomization. The QKD offers unrestricted transmission of secure keys among two distant parties. They suggest a hybrid extent attack with homodyne detection, rectilinear optic modes, and single photon detection, allowing a vacuum-based weak decoy state QKD-based system to be used. At the same time, the source phases are moderately randomized, and the listeners can hack the data about key customers' revealed information [18]. The author Mayers D described the unconditional security of QKD and reviewed the basic principles and supporting philosophies used to implicate any QKD protocol [19]. Hoi-Kwong Lo et al. proposed the non-provisional protection of QKD over randomly extensive distances. The QKD over ALD of a proper noisy channel made it accurately secure. They

used traditional possibilities theory to convert a loud quantum scheme (QS) to a noiseless QS and then from a noiseless QS to a noiseless conventional QS [20].

Author Barrett J has described standard QKD protocols used to secure against snooping types of attacks and a QKD scheme testable to secure against all-purpose cyber malware injectors by a PQC listener who is a restricted individual by the impossible mechanism of superluminal signalling [21]. The author, G. Brassard, described the QuCr approach as providing security and privacy to permit two end-node enterprises to interconnect with testable faultless secrecy under a listener's nose and brilliant with limitless computational power [22]. The QuCr is a security extension principle that uses the ideologies of quantum mechanics to encrypt data and transmit, which is impossible to hack. QuCr is the resolution to protect and imminently prove private penetrating data [23]. Author Zhang B et al. proposed a quantum network (QN) with arbitrary failures and intentional-level cyber malware injectors. It has described key functionalities of QNs in a circulated quantum data processing environment. The unexpected random breakdown type of network errors and intentional level cyber malware injectors are predictable according to the increment of size of the network, so it is significant to appreciate the robustness of a huge-scale QN. It also described error incidences in exponential QNs: error purely re-parameterized QNs, Waxman QNs, which lead to quantum capacity linear decrease consequences with measurements of error possibilities [24].

The author Yang Yang et al. have proposed a compressive cloud environmental data secure storage protocol that simulates the Goldreich-Goldwasser-Halevi CSs approach. Meanwhile, the accumulated blocks can be recreated from combined integrated patch-tags without data catalogues, and the cloud environment implicates collecting data patch-tags for delivering the confirmable veracity evidence. It helps to reduce data storage, transmission costs, and end-user privacy [25]. Stefanie Barz has described blind QC, which presents significant computational speedups and is expected to preserve computational privacy. The approach has built the input, output, and computations unknown to the computers and end-users. It has exploited the theoretical context of measurable quantum calculations, which authorizes consumers to envoy an estimate to a quantum distributed server. It also presented many other blind vicarious measures, such as 1-qubit and 2-qubit logical gates, along with Deutsch and Grover quantum algorithmic sequences [26].

Amiri R et al. proposed QDS structures extensively used in current data transmission channels to assure transferability and data authenticity. These are treated as alternative classical schemes that rely on computational assumptions without the involvement of trusted quantum media. It shows that the threshold of quantum channel noise for the QDS structure is less strict than for refining a key in security mode. They imply QKD and describe the direct QDS schemes that are preferable to signature structures that rely on undisclosed collective keys produced by [27].

Thornton M et al. proposed continuous variable QKDs over insecure channels. The QKDs confirm the truth of conventional data communication and the sender's validity. The modern communication channels implicated with supporting signature structures depend on computational conventions, which reduce insecurity by QC; the continuous variable system trusts on the segment extent of a scattered alphabet of intelligible states, and it consents for secure data validation and verification in contradiction to a quantum adversary accomplishment cooperative beam splitter and tangling-cloner cyber malware injectors. Since CVS is built on quantum channels with a shorter signature than preceding protocols with no listener, it opens the opportunity to execute CVS QDKs together with prevailing CVS QKD platforms with minimal modification [28]. Hong-Xin Ma et al. proposed long-distance CVS measurement-device-independent QKD with a protocol with discrete modulation (DM), which

provides good compatibility with a well-organized fault rectification encoder with a decoder that controlled innovative reconciliation proficiency uniformly at a short level of signal-to-noise ratio. The planned protocol is protected in contradiction to random collective cyber malware injectors on asymptotic edges with appropriate decoy state utility. With DM, the designed approach-based protocol outperforms earlier protocols regarding the maximum communication distance that can be reached. They solved the problem of the innovative Gaussian-modulated long-distance CVS measurement-device-independent QKD protocol [29].

The author, Shetu SF et al. [30], proposed an analysis of botnet implications in the cyber security field. They described in detail the categories of all feasible botnet detection procedures by analyzing formerly distributed findings, methodologies, and updated innovations in cyber security. The authorization, authentication, and access control mechanisms are vital in secure data transmission. The author Henge SK et al. [31] proposed a fully homomorphic encryption methodology-based blended approach that has unified the multi-feature-data-matrices-authentication–authorization process with reliable and non-reliable parameters, which are integrated to provide altering system and security-privacy for tenants using enhanced homomorphic CSs and Brakersky–Gentry–Vaikuntanathan (BGV) structure.

Unauthorized users, external sources listening in on the network, and internal users giving away the store all threaten the integrity and privacy of data. A few complicated security threads and issues will damage the data security environment, such as code injections, falsifying end-user identities, malicious bots, eavesdropping and data theft, data tampering, unauthorized access to tables, columns, and data rows, scaling the security administration of multiple systems, low-level user access control, and so on [32]. Blockchain (BC) is a new generation of secure information technology fueling business, enterprise, and industrial modernization. Researchers proposed approaches and methodologies for key facilitating technologies for resource organization and system operation in a BC-secured smart manufacturing environment in Industry 4.0. It described BC system integrations to overcome potential cybersecurity challenges and achieve intelligence in Industry 4.0. It has analyzed eight cybersecurity issues and addressed ten metrics for implementing BC application data in the manufacturing of environmental devices [33].

BC is an evolving standard of secure and shareable computing environments, which are an organized combination of chain structure for data storage and verification, scattered consent algorithms for producing and modernizing data, cryptographic practices for ensuring end-to-end data broadcast and access control-based security, and computerized smart conventions for data programming and operational tasks. It articulated BC security-based research at three levels: process, data, and infrastructure [34]. Another study described the transparency qualities enabled by BC, which implies the attractive sustainability of manufacturing networks. It described the 12 metrics of accepting BC in the manufacturing industry, which concluded by relating to nine blocks of the Business Model Canvas [35]. Digital twin technology (DT) attracted incredible attention in its early years. A minimal Google search task on DT produces over 2.4 billion results. The DT association distinguishes a DT as an adequate interpretation of the practical mode of systems and activities coordinated at an identified rate and reliability [36]. The DT functionalities are considered model-based systems engineering. The DTT advances through four dimensions: definition, coverage, technology, and scalability.

DTs are digital clones of physical systems that can quickly construct data centres (DCs). However, they increase a DC's attack surface and prepare opponents with critical levels of accessibility [37]. The DTs methods propose different perceptions for selecting the context of information equipment and

intelligent production systems [38]. Risks of DTs in DCs, unauthorized access to DTs can cause substantial security risks. The attackers could obtain access credentials to DC's stored data if DCs DTs negotiated. Another author has focused on highly effective defect diagnosis methods, low-price, high-cost devices, and low efficiency to attain well-timed response and precise fault detection solutions and protect manufacturing systems (MS). It asserted that hybrid IoT with DTT has been integrated to investigate the consequences of flaws discovered competently predicted and secures the MS. Another piece of research has stated that the industry's production control of R and D-stage products for the mass individualization paradigm is difficult due to the frequently disturbed environment and mix flow. With the merging of the maintainable development goals and the mounting customized demands in manufactured goods, durable manufacturing is imagined in Industry 5.0. The author projected a BC smart contract pyramid-driven multi-agent autonomous process control environment [39]. In another piece of research, the author proposed Maker-chain, a new decentralized blockchain-driven model to manage the social manufacturing cyber-credits between various makers. It has used chemical signatures-based anti-counterfeiting techniques to denote unique features of personalized products [40].

P. Dhiman et al. proposed a Block chain-Merkle-tree Ethereum approach in an enterprise MT cloud environment (CE). It highlights using CE-MT with blockchain (BC) to increase security and privacy in CE. It has implicated cypher-text policy attribute encryption algorithmic sequences through various levels of MT, such as inner, outer, Inner-Outer-External, Outer-Inner, and External-Outer-Inner and stated that it achieved 92 of validity and data access control (DAC) [41]. The same author has proposed another approach to the implications of the secure token key using Brakersky-Gentry-Vaikuntanathan (BGV) hybrid HE. They are processed through multi-factor authentication and authorization modes. They tested with 152 end-users by integrating six multi-tenants, five head tenants, and two enterprise levels. The author, P. Dhiman, proposed qualified scrutiny complications in cloud security and non-homomorphic and HE practices. It has described several proposed methods and approaches with pros and cons concerning CC security [42]. The same author has presented a study of blockchain-based secure models and advances based on different CMT services. It stated the few passages of blockchain with the integration of HE methods which help to build a robust security system in an MT environment [43].

The following complexities are identified through the analytical in-depth research survey:

- Modern TLS handshakes and ciphertexts have been stored in classic public-key encryption and are formed into middleware; this environment allows attackers to track the stored keys integrated with unique session-key wares salted-key operating systems and to decrypt the following individual ciphertext systems [44]. The middleware-stored ciphertexts cannot be secure even when synchronizing with forward-security methods.
- Creating security key scenarios and forward-security-ciphertexts is challenging due to the technical feasibility of securing the data in transit, storage, user, and server modes.

This study proposes using quantum computing to distribute security keys using the post-quantum cryptography mathematical algorithm. It presents security scenarios with technical feasibility for securing data in transit, storage, user, and server modes. Post-quantum cryptography has framed and implicated the mathematical algorithm used to generate the secure key distributed along with the data in transit, storage, and editing mode. It has involved reversible computations on many different numbers by super positioning the qubits to provide quantum services and other product-based cloud-online access used to process the end-users of artificial intelligence-based hardware service components.

3. Methodology

The quantum secret sharing (QSS) component environment in the distributed multi-tenant environment efficiently involves certain level computations between various untrusted groups of people [7].

3.1. Quantum-based secret sharing (QbSS)

The quantum states with shared private keys demonstrate the technical feasibility of secure communication among untrustworthy groups in distributed multi-tenant environments. The QbSS design facilitates sharing specific quantum keys by using quantum cryptographic protocols (QCP) and quantum-based key distributions. It will support quantum computation in secure distributed computations [7].

3.2. Post-quantum cryptography (PQC) implications with four phases of execution

Existing PuK-CSs rely on integer factorization (IF) and discrete-logarithm (DL) problems [45]. To solve IF and DL problems, post-quantum cryptography (PQC) is proposed with Shor's algorithm [16–18]. Quantum technicality is a mathematical schema with internal rules for developing physical hypotheses. The PQC is associated with cryptosystems that can be run on standard computers to secure data against cyber-malware injectors by QC [7].

Many cryptographers are researching and developing new crypto algorithms for QC systems to avoid future hazards. In contrast, most existing symmetric cyphers and hash functions resist quantum computers. The algorithmic implications of the quantum-based Grover are increasing cyber-attacks against symmetric cyphers in symmetric cryptography, but it neutralizes the growing size of the key. PQC's mathematical schema is unrelated to generalized symmetric algorithms, and it differs from QuCr, but it will use quantum-based occurrences to achieve secrecy and privacy. The PQC is involved in all four phases, as shown in Figure 2.

The complete post-quantum cryptography (PQC)-based optimization performances with the four phases are shown in Figure 2. The first stage of the cryptographer's environment (CE), the primary layer for the sender and receiver, is provided by Phase-I. The CE is involved in various CE operations that use single, multiple, or blended data encryption standards and AES techniques such as TDEA, Nth-Degree Truncated Polynomial Ring (NDTPR), Merkle-Hellman Knapsack Encryption, Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm, and McEliece Encryption. The sender's data has been encrypted using a combination of techniques and then supplemented with secure signatures more suitable for the verification mode.

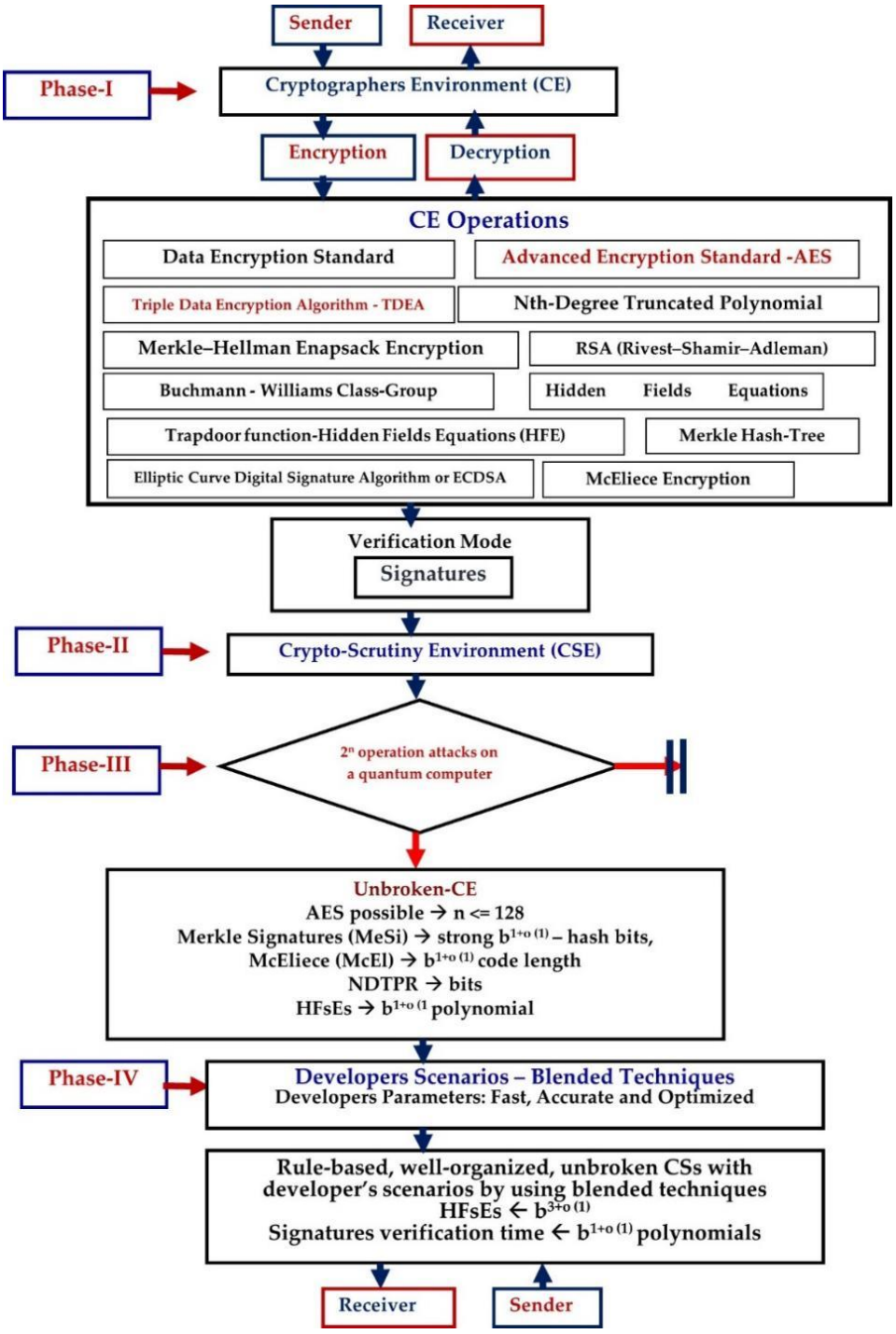

Figure 2. Post-quantum cryptography (PQC) based optimization performances with the four levels of execution.

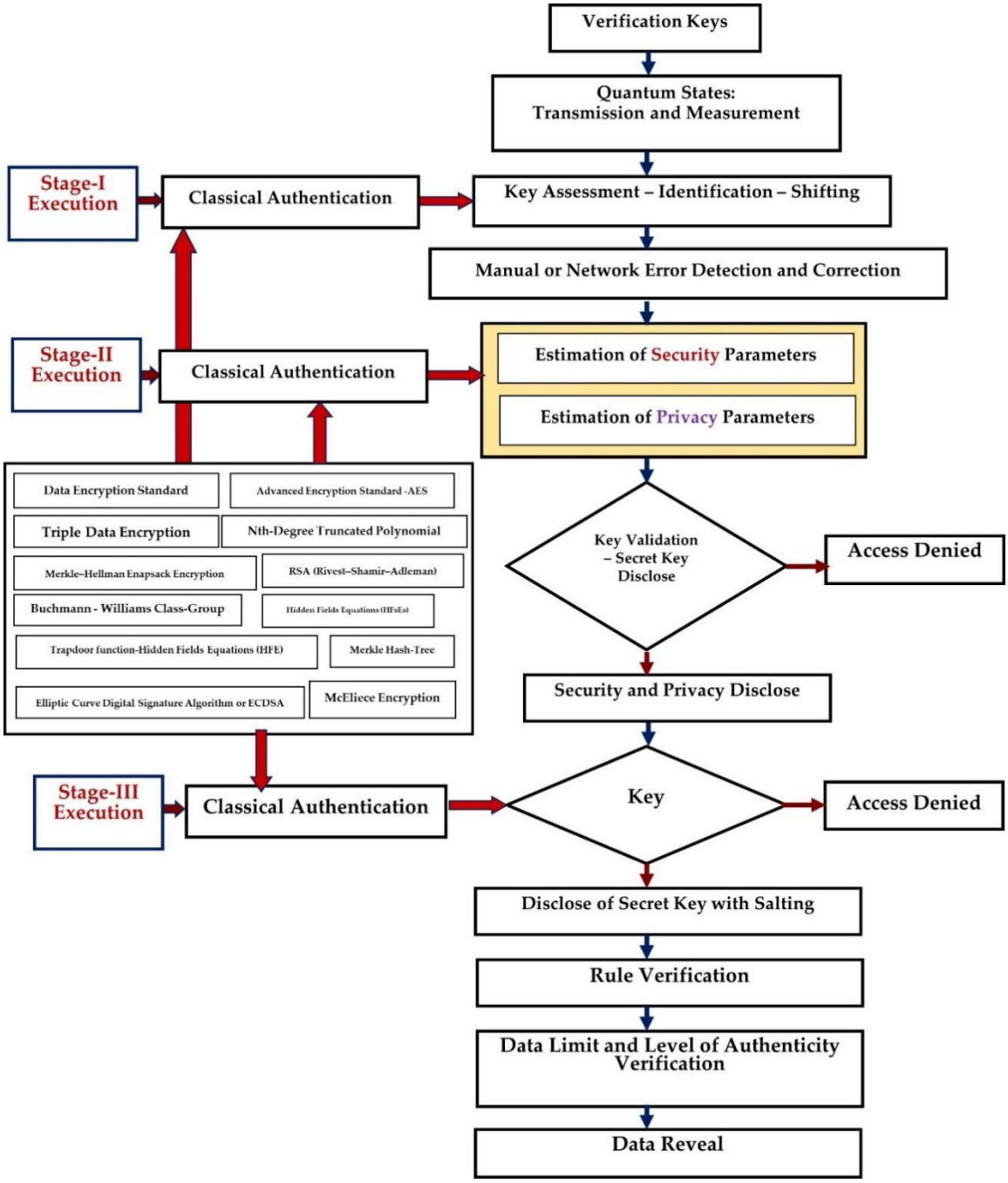

Figure 3. Distribution of secure keys through the PQC mathematical algorithm.

The sender's data, including signature and crypto-keys, is then sent to the crypto-scrutiny Environment (CSE), considered phase II. The CSE was scrutinized with various validations in Phase II before being sent to Phase III. Phase III was tested on a quantum computer with multiple test cases using 2n operation attacks. In addition, compromising the authenticity is difficult due to the intense level of Quantum security, which is prepared with various blended quantum states of crypto techniques, such as

AES possible → n <= 12

Merkle Signatures (MeSi) → strong b1+o (1) – hashing bits,

McEliece (McEl) → b1+o (1) code length

NDTPR → bits

HFsEs → b1+o (1) polynomials

After the implications of test cases in phase III, the developers' scenarios have been activated with developer's parameters such as accurate, fast, and optimization techniques in phase IV, as shown in Figure 3. The phase-IV is proving the Rule-based, well-organized, unbroken CSs with developer's scenarios by using blended techniques such as

HFsEs ← b3+o (1)

Signatures verification time ← b1+o (1) polynomials

Finally, the reverse scenarios can be executed from sender to receiver to receive the data successfully.

4. Experimental scenario and analysis

The PQC with mathematical framework computations is categorized into the three family clusters such as code-implicated-cryptosystems (CICSs), lattice-implicated-cryptosystems (LICSs), and multivariate-implicated-cryptosystems (MVICSs). Along with these three, there are other cluster groups with these major cluster groups [46].

- Post-quantum cryptography with quantum key distribution (QbKD) mathematical framework computations are framed through the CIC, LIC, and MVIC, which are blended with various combinations to avoid attacks and data leakage; if the cluster group gets failure, other cluster groups can take charge to protect the data and environment. The CIC, LIC, and MVIC hold different functionalities for showing the potential sources of statistical complexity. The LIC is designed in the form of lattices treated as geometric structures, represented by matrices framed by mathematical arrays.
- The CIC is majorly implicated with the error detection and error-correction codes specifically used for data security.
- The MVIS depends on solving a quadratic polynomial-based system with equations over a finite field.

The parameter generation at various levels in a DoSK using the PQC-based algorithm is described in Table 1. T stands for access tree, PuK stands for the public key, SK stands for the secret or private key, M stands for the message, CT stands for cypher text, and N stands for node in a tree. The token key is used for Internal-Global and Global-Internal tenant setup. Because only token keys can be used for internal communication, no additional vital combinations are required for global communication. In such communications, an extra key containing the token key is sent along with the packets. To encrypt packets in the sender enterprise, tokens, salting, and public keys are used. A secure key is added to send packets to another enterprise tenant. A combination of the token, salting, public key, private key, secret key, cypher text, and N-based are used. Communication is done locally for Internal-External and External-Internal tenant setup, so an additional key is not required. Token keys are sufficient for security. Salting is used with token keys to provide extra protection for all other tenant setups, and a multi-factor authentication mechanism is used here.

Table 1. The distribution of secure keys-based parameters is considered for accessing the data in transmit storage, user, and server mode.

End-User Type	Tenant Type	Environment Type	Implicated Tokens and Keys	Encryption Consequences	Decryption Consequences	Mediation Layer Supporting Keys
Senders Environment	Inner-Outer-External Tenant	Internal-External-Global-Global	Token + Salting + PuK + M + T based	Token + Salting + PuK + M + T based	Token + Salting + CT + SK + N based	Token + Salting + PuK + M + T + CT + SK + N based
	Inner-Outer-Tenant	Internal-External-Global	Token + Salting + PUK based	Token + Salting + PuK based	Token + Salting + CT + SK based	Token + Salting + PuK + M + T + CT based
	Outer Tenant	External-Global	Token + Salting based	Token + Salting based	Salting + Token + CT based	Token + Salting + CT based
	Inner-Tenant	Internal-External	Token-based	Token-based	Token-based	Token-based
	Sender Tenant	Internal-Global	Token, PuK, M, T	Token, PuK, M, T	CT, SK, N, Token	PuK, M, T
Receivers Environment	Receiver Tenant	Global-Internal	PUK, M, T, Token	CT, SK, N	Token, CT, SK, N	PuK, M, T
	Inner-Tenant	External-Internal	Token-based	Token-based	Token-based	Token-based
	Outer Tenant	Global-External	Salting + token based	Salting + token based	CT + Token + Salting based	CT + Salting + Token based
	Outer-Inner-Tenant	Global-External-Internal	PuK + Salting + Token based	PuK + Salting + Token based	SK + CT + Salting + Token based	CT + T + M + PuK + Salting + Token
	External-Outer-Inner Tenant	Global-Global-External-Internal	T + M + PuK + Salting + Token	T + M + PuK + Salting + Token	N + SK + CT + Salting + Token Based	N + SK + CT + T + M + PuK + Salting + Token based

The QbKD has the advantage of unconditional secure pathways for allocating specific arbitrary keys using secure, trusted channels. The QbKD involved keys generated and then used in encryption algorithmic sequences to improve data security-privacy. It demonstrates the tool's security by allowing secure keys with an authenticated agreement to pass through untrusted pathway channels where the output key is exclusively self-determining from any input value. This task is impracticable using standard cryptography techniques. The QbKD is involved with the help of classical cryptography techniques with new security parameters as classical authentication in every stage of execution, such as stage 1, stage 2, and stage 3 level of performances, as shown in Figure 2, Figure 3, and Table 1. The keys are generated, verified, and passed to quantum states with their internal measurement. Stage 1 can be involved in key evaluations, identify co-related properties and parameters, and shift some internal adjustable rules using classical authentication. Manual network errors can be detected and corrected for more secure execution.

5. Results and discussion

The proposed model employs a mathematical post quantum cryptography-based methodology to secure data while in transit, storage, and end-user mode, such as sender or receiver, with the provision of multi authentication and authorization processes. The proposed algorithmic based key sequences such as generation time (GT), encryption time (ET) and decryption time (DT) are illustrated in Figures 4 and 5. The encryption and decryption schemes are implicated in this research based on the end-user, tenant type, role, data position mode such as transition, storage, or end-user level, and environment types. The key-generation mechanism will integrate and initiate itself based on end-user, tenant type, role, data position mode such as transition, storage, or end-user level, and environment type. When the

end-role user's is guest, insider, trusted, outsider, permanent, anonymous, or temporary, the post quantum cryptography-based methodology sequences are automatically applied. In addition, the implications of proposed post-quantum encryption algorithmic based key sequences such as GT, ET and ET levels are illustrated in Figure 6. When the user type is insider or insider-tenant, post quantum cryptography techniques such as private, public, and salting are initiated, and when the user type is guest, trusted, outsider, and permanent, anonymous, and temporary, post quantum cryptography techniques such as private, public, and salting are initiated. Outsiders are divided into two categories: Trusted Outsiders and Un-Trusted Outsiders.

Quantum techniques are used to generate the PuK and SKs for a Trusted Outsider and a guest user. Guest users are thought to be more vulnerable to breaches because the risk is higher in this case. A hybrid key is generated for an Un-trusted Partial category using a post-quantum techniques algorithm. The dictionary mechanism has been used to store and track end-user records. Any new user gets an entry in the dictionary. The dictionary stores the IP address, system location, name, and some other details. When an attacker attempts to access the data, the IP address is traced using the dictionary, and self-key mutation occurs to protect the data from unauthorized access. The proposed methodology has been tested using 16 to 32-byte key formations, as well as a number of parity rules designed with self-key-transformation-techniques with a number of 0's and 1's.

The API-web interface with cloud integration was designed using the Xampp server-based cross-platform environment. Tenant-level, multi-tenant-level, and cloud-tenant-level servers are included, as well as a database server. In the proposed model, the tomcat server is used as a web server, and the dictionary integration of MySQL is used. This model is designed for four enterprises with 245 users, and it employs integration parity rules that are implemented using salting techniques.

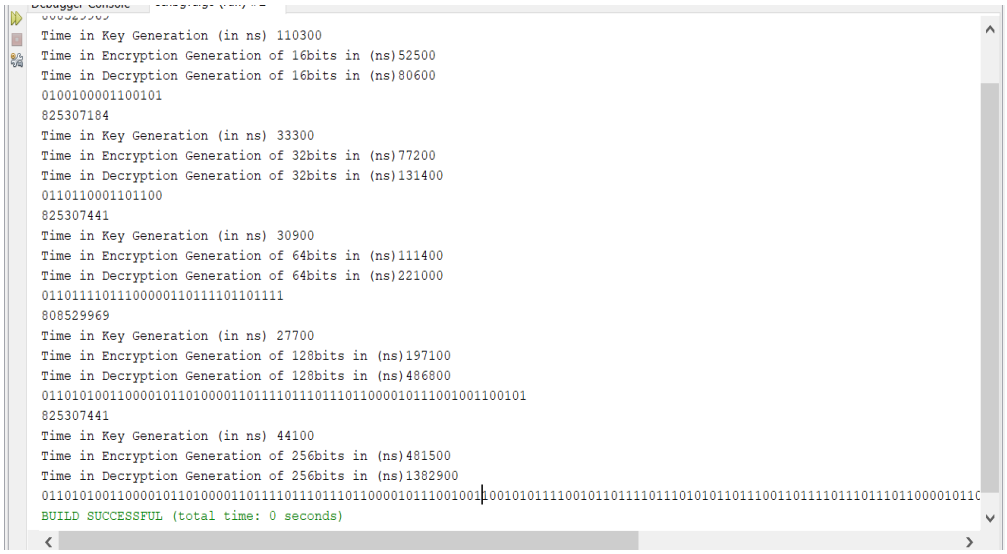

Figure 4. Implications of proposed algorithmic basic level sequences based key sequences such as generation time (GT), encryption time (ET) and decryption time (DT).

Figure 5. Implications of proposed algorithmic-based key sequences such as GT, ET and ET levels.

Figure 6. Implications of proposed post-quantum encryption algorithmic-based key sequences such as GT, ET and ET levels.

5.1. Data distribution key generation time variations in transit, storage and end-user modes

The mathematical post quantum cryptography-based methodology has implicated various secure keys for data distribution to secure the data while it is in transit-mode, storage-mode and end-user mode as shown in the Table 2 and Figure 7. The data distribution and key generation time in quantum-level 2 is less as compared to the quantum-level 1 since a quantum-level 2 holding back-execution caching mechanism, which helps the localized and distributed networks to secure the data while it is in transit, storage, and end-user mode.

Table 2. Mathematical post-quantum cryptography-based methodology to implicate secure keys data distribution key generation time variations in transit, storage, and end-user modes.

Key Size	Quantum-Level 1 (in ms)	Quantum-Level 2 (in ms)
24 bits	0.509	0.5025
72 bits	5.09	0.1954
128 bits	5.09	0.1766
256 bits	5.09	0.2261
1024 bits	5.09	0.233
2048 bits	5.09	0.1211
4096 bits	5.09	0.2239
8248 bits	5.09	0.1099

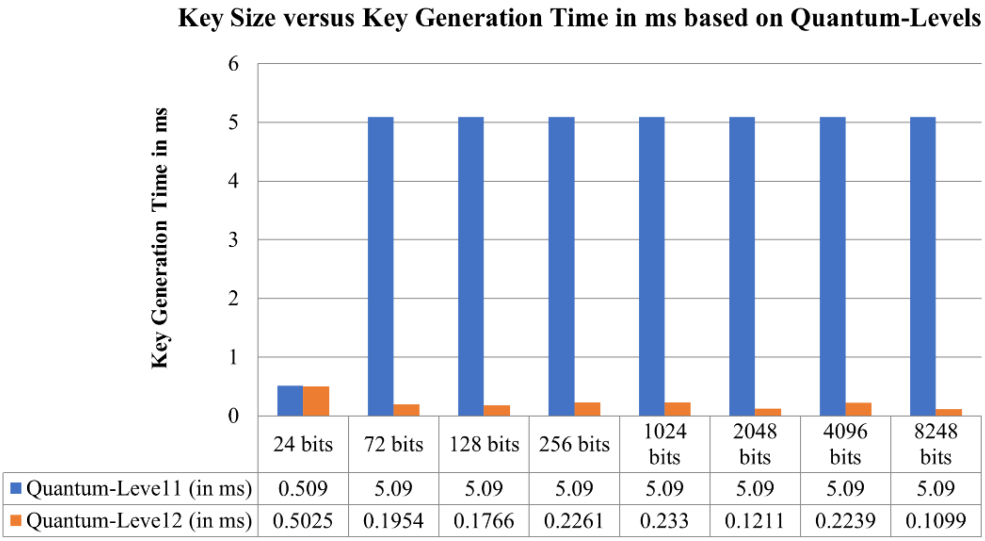

Figure 7. Mathematical post-quantum cryptography-based methodology to implicate secure keys data distribution key generation time variations in transit, storage and end-user modes.

5.2. Data distribution key generation encryption time variations based on plain text

The data distribution to secure the data and their generation encryption time variations based on plain text with the integration of transit-mode and end-user mode as shown in the Table 3 and Figure 8.

Table 3. Mathematical post-quantum cryptography-based methodology to implicate secure keys data distribution key generation encryption time variations based on plain text.

Plain Text Size	Quantum-Leve1 1 (in ms)	Quantum-Leve1 2 (in ms)
24 bits	2.3233	0.0355
72 bits	3.1756	0.0863
128 bits	3.8193	0.113
256 bits	4.9124	0.1493
1024 bits	6.0552	0.3443
2048 bits	7.2221	0.7684
4096 bits	7.8624	1.1374
8248 bits	8.7277	1.8491

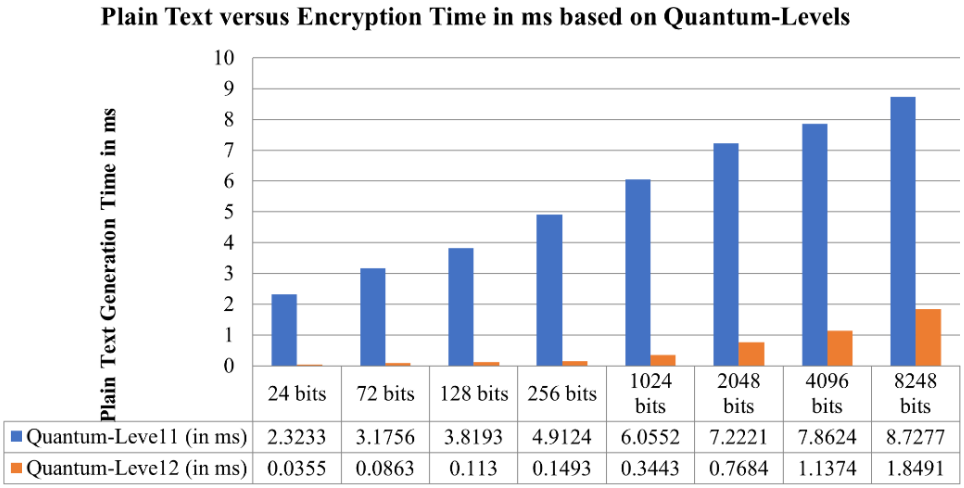

Figure 8. Mathematical post-quantum cryptography-based methodology to implicate secure keys and data encryption time variations based on plain text.

5.3. Data distribution key generation decryption time variations based on plain text

This section discusses the time taken to process the decryption according to the plain text information with various secure keys for data distribution to secure the data. The generation decryption time variations based on plain text with respect to the integration of transit-mode and end-user mode as shown in the Table 4 and Figure 9.

Table 4. Mathematical post-quantum cryptography-based methodology to implicate secure keys data distribution key generation decryption time variations based on plain text.

Plain Text Size	Quantum-Leve1 1 (in ms)	Quantum-Leve1 2 (in ms)
24 bits	2.1533	0.0525
72 bits	4.1264	0.1582
128 bits	6.2627	0.3305
256 bits	8.6085	0.6308
1024 bits	11.4445	0.8546
2048 bits	14.0209	2.407
4096 bits	16.8254	2.6386
8248 bits	19.4799	3.3513

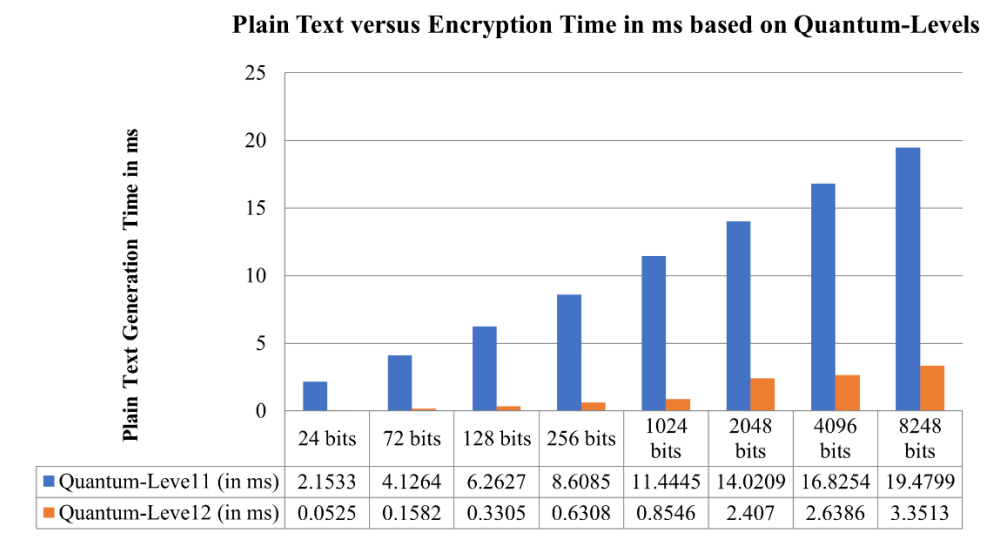

Figure 9. Mathematical post-quantum cryptography-based methodology to implicate secure keys and data decryption time variations based on plain text.

Hence, the proposed hybrid approach is better regarding key GT and ET. Therefore, it can be determined that the proposed model is better in terms of providing better security. The time required for generating the keys, encryption, and decryption is significantly less than the EHC algorithm.

6. Conclusions

Quantum computing efficiently processes the composite algorithms, allowing for innovative advances in cyber security, forensics, artificial intelligence, and machine learning-based complex systems. It also demonstrates solutions to many challenging problems in cloud computing security. This study proposes using quantum computing to distribute security keys using the post-quantum cryptography mathematical algorithm. It suggests security scenarios and technical options for securing data in transit, storage, user, and server modes. Post-quantum cryptography has framed and implicated the mathematical algorithm in generating the distributed secure key alongside the data-in-transit, data-

storage, and data-editing methods. It has involved reversible computations on many different numbers by super positioning the Qubits in providing quantum services and other product-based cloud-online access used to process the end-user's artificial intelligence-based hardware service components. This study will be helpful to researchers and industry experts to develop specific scenarios to synchronize their data with cloud servers in medicine, finance, engineering, and banking. Post-quantum computing-based critical distribution planning will be used in future work to execute multi-tenants of various enterprises for internal and external secure communication.

Acknowledgements

This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/215), Taif University, Taif, Saudi Arabia.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. W. S. Peter, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, **26** (1997). https://doi.org/10.1137/S0097539795293172
2. W. Zhao, R. H. Shi, J. J. Shi, X. C. Ruan, Y. Guo, D. Huang, Quantum digital signature based on measurement-device-independent continuous-variable scheme, *Quantum Inf. Process.*, **20** (2021), 222. https://doi.org/10.1007/s11128-021-03152-7
3. Montanaro, Ashley, Quantum algorithms: an overview, *npj Quantum Inf.*, **2** (2016), 15023. https://doi.org/10.1038/npjqi.2015.23
4. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, Demonstration of blind quantum computing, *Science*, **335** (2012), 303–308. https://doi.org/10.1126/science.1214707
5. X. Tan, Introduction to quantum cryptography, in *Theory and Practice of Cryptography and Network Security Protocols and Technologies* (eds. J. Sen), Rijeka: IntechOpen, 2013. https://doi.org/10.5772/56092
6. D Stebila M, Moscaand N Lütkenhaus, The case for quantum key distribution, in *Quantum Communication and Quantum Networking* (eds. A. Sergienko, S. Pascazio and P. Villoresi), Berlin, Heidelberg: Springer, **36** (2010). https://doi.org/10.1007/978-3-642-11731-2-35
7. S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scaran, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.*, **11** (2019), 045021. https://doi.org/10.1088/1367-2630/11/4/045021
8. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, et al., Advances in quantum cryptography, *Adv. Opt. Photonics*, **12** (2020): 1012–1236. https://doi.org/10.1364/AOP.361502
9. I. S. Kabanov, R. R. Yunusov, Y. V. Kurochkin, A. K. Fedorov, Practical cryptographic strategies in the post-quantum era, *AIP Conf. Proc.*, **1936** (2017), 020021. https://doi.org/10.1063/1.5025459

10. D. A. Kronberg, E. O. Kiktenko, A. K. Fedorov, Yu. V. Kurochkin, Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack, *Quantum Electron.*, **47** (2017), 163–168. https://doi.org/10.1070/QEL16240
11. Serious Security: Post-Quantum Cryptography (and why we're getting it), 2023. Available from: https://nakedsecurity.sophos.com/2019/02/07/serious-security-post-quantum-cryptography-and-why-we-are-getting-it.
12. E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, A. K. Fedorov, Symmetric blind information reconciliation for quantum key distribution, *Phys. Rev. Appl.*, **8** (2017), 044017. https://doi.org/10.1103/PhysRevApplied.8.044017
13. B. Huttner, L. Perret, Quantum-Safe Security, Working Group Overview, Available from: https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security.
14. K. Hirapara, The need to be quantum-safe-cyber security threats in the era of quantum computing, Vtech Solution, 2018. Available from: https://www.vtechsolution.com/why-the-need-to-be-quantum-safe-the-era-of-quantum-computing.
15. The advantages and disadvantage of quantum computing, 2018. Available from: https://www.e-spincorp.com/the-advantages-and-disadvantage-of-quantum-computing.
16. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, 26 (1997), 1484. https://doi.org/10.1137/S0097539795293172
17. D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography* Berlin, Heidelberg: Springer, (2009), 1–14. https://link.springer.com/chapter/10.1007/978-3-540-88702-7_1
18. S. H. Sun, M. S. Jiang, X. C. Ma, C. Y. Li, L. M. Liang, Hacking on decoy-state quantum key distribution system with partial phase randomization, *Sci. Rep.*, **4** (2014), 4759. https://doi.org/10.1038/srep04759
19. D. Mayers, Unconditional security in quantum cryptography, *J. ACM*, **48** (2001), 351–406. https://doi.org/10.1145/382780.382781
20. H. K. Lo, H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, **283** (1999), 2050–2056. https://doi.org/10.1126/science.283.5410.2050
21. J. Barrett, L. Hardy, A. Kent, No signaling and quantum key distribution, *Phys. Rev. Lett.*, **95** (2005), 010503. https://doi.org/10.1103/PhysRevLett.95.010503
22. G. Brassard, Brief history of quantum cryptography: a personal perspective, *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Awaji, Japan, (2005), 19–23. https://doi.org/10.1109/ITWTPI.2005.1543949
23. Implementing quantum-safe key distribution, 2021. https://quantumxc.com/quantum-cryptography-explained.
24. B. Zhang, Q. Zhuang, Quantum internet under random breakdowns and intentional attacks, *Quantum Sci. Technol.*, **6** (2021), 045007. https://doi.org/10.1088/2058-9565/ac1041
25. Y. Yang, Y. J. Chen, F. Chen, A compressive integrity auditing protocol for secure cloud storage, *IEEE ACM Trans. Netw.*, **2** (2021), 1197–1209. https://doi.org/10.1109/TNET.2021.3058130
26. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, Demonstration of blind quantum computing, *Science* **335** (2012), 303–308. https://doi.org/10.1126/science.1214707
27. R. Amiri, P. Wallden, A. Kent, E. Andersson, Secure quantum signatures using insecure quantum channels, *Phys. Rev. A*, **93** (2016), 032325. https://doi.org/10.1103/PhysRevA.93.032325

28. M. Thornton, H. Scott, C. Croal, N. Korolkova, Continuous-variable quantum digital signatures over insecure channels, *Phys. Rev. A*, **99** (2019), 032341. https://doi.org/10.1103/PhysRevA.99.032341
29. H. X. Ma, P. Huang, D. Y. Bai, T. Wang, S. Y. Wang, W. S. Bao, Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation, *Phys. Rev. A*, **99** (2018), 022322. https://doi.org/10.1103/PhysRevA.99.022322
30. S. F. Shetu, M. Saifuzzaman, N. N. Moon, F. N. Nur, A survey of botnet in cyber security, in *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, IEEE, Jaipur, India, (2019), 174–177. https://doi.org/10.1109/icct46177.2019.8969048
31. P. Dhiman, S. K. Henge, R. Ramalingam, A. Dumka, R. Singh, A. Gehlot, et al., Secure token-key implications in an enterprise multi-tenancy environment using BGV–EHC hybrid homomorphic encryption, *Electronics*, **11** (2022), 1942. https://doi.org/10.3390/electronics11131942
32. Data security challenges, 2023. Available from: https://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm.
33. J. W. Leng, S. D. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, et al., Blockchain-secured smart manufacturing in industry 4.0: A survey, *IEEE Trans. Syst. Man Cybern. Syst.*, **51** (2021), 237–252. https://doi.org/10.1109/TSMC.2020.3040789
34. J. Leng, M. Zhou, J. L. Zhao, Y. Huang, Y. Bian, Blockchain security: a survey of techniques and research directions, *IEEE Trans. Serv. Comput.*, **15** (2022), 2490–2510. https://doi.org/10.1109/TSC.2020.3038641
35. J. W. Leng, G. L. Ruan, P. Y. Jiang, K. L. Xu, Q. Liu, X. L. Zhou, et al., Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey, *Renew. Sust. Energ. Rev.*, **132** (2020), 110112. https://doi.org/10.1016/j.rser.2020.110112
36. Gaurav Gupta, Digital Twin: A Foundation for a Secure, Intelligent and Connected Enterprise, https://isg-one.com/articles/digital-twin-a-foundation-for-a-secure-intelligent-and-connected-enterprise.
37. Maria Korolov, How to secure digital twin technology in your data center, 2022. Available from: https://www.datacenterknowledge.com/security/how-secure-digital-twin-technology-your-data-center.
38. L. Gopal, H. Singh, P. Mounica, N. Mohankumar, N. P. Challa, P. Jayaraman, Digital twin and IOT technology for secure manufacturing systems, *Meas.: Sens.*, **25** (2023), 100661. https://doi.org/10.1016/j.measen.2022.100661
39. J. W. Leng, W. Sha, Z. S. Lin, J. B. Jing, Q. Liu, X. Chen, Blockchained smart contract pyramid-driven multi-agent autonomous process control for resilient individualized manufacturing towards Industry 5.0, *Int. J. Prod. Res.*, (2022), 1–20. https://doi.org/10.1080/00207543.2022.2089929
40. J. W. Leng, P. Y. Jiang, K. L. Xu, Q. Liu, J. L. Zhao, Y. Y. Bian, et al., Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing, *J. Clean. Prod.*, **234** (2019), 767–778. https://doi.org/10.1016/j.jclepro.2019.06.265
41. P. Dhiman, S. K. Henge, S. Singh, A. Kaur, P. Singh, M. Hadabou, Blockchain merkle-tree ethereum approach in enterprise multi-tenant cloud environment, *Comput. Mater. Contin.*, **74** (2023), 3297–3313. https://doi.org/10.32604/cmc.2023.030558
42. P. Dhiman, S. K. Henge, Comparative analysis of cloud security complexities and past proposed non-homomorphic and homomorphic encryption methodologies with limitation, in *ICT for Competitive Strategies*, Boca Raton: CRC Press, (2020), 787–799.

43. P. Dhiman, S. K. Henge, Analysis of blockchain secure models and approaches based on various services in multi-tenant environment, in *Recent Innovations in Computing*, Singapore: Springer, **855** (2022), 563–571. https://doi.org/10.1007/978-981-16-8892-8_42
44. K. Kwiatkowski, Towards post-quantum cryptography in TLS, 2019. Available from: https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls.
45. C. Meshram, S. A. Meshram, An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem, *Inf. Process. Lett.*, **113** (2013), 375–380. https://doi.org/10.1016/j.ipl.2013.02.009
46. NIST reveals 26 algorithms advancing to the post-quantum crypto 'semifinals', 2019. Available from: https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals.

AIMS Press