Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P.5654-5663 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Quantum Computing and Its Implications for Cryptography: Assessing the Security and Efficiency of Quantum Algorithms

Ashish Jain[1], Dr. RVS Praveen[2], Vinayak Musale[3], Narender Chinthamu[4], Yogendra Kumar[5], Dr. B V RamaKrishna[6], Dr. Anurag Shrivastava[7]

[1]Department of Computer Science and Engineering, SSET, Sharda University, Greater Noida
[2]Director Product Engineering, Digital Engineering and Assurance, LTIMindtree Limited, M/s. Divija Commercial Properties, Serlingampally Mandal, Hyderabad, Telangana, 500081
[3]Assistant Professor, Department of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India
[4]Senior, Enterprise Architect, MIT CTO, Dallas, Texas, USA
[5]Department of Electrical Engineering, GLA University, Mathura, India
[6]Associate Professor, Aditya College of Engineering and Technology, Surampalem, Kakinada, India
[7]Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,
Chennai, Tamilnadu

How to cite this article: Ashish Jain, RVS Praveen, Vinayak Musale, Narender Chinthamu, Yogendra Kumar, B V RamaKrishna, Anurag Shrivastava (2024) Quantum Computing and Its Implications for Cryptography: Assessing the Security and Efficiency of Quantum Algorithms. *Library Progress International*, 44(3), 5654-5663.

Abstract
Quantum computing is a new type of computing that is revolutionizing the kind of computational power at people's disposal, including their cryptography applications. This paper aims at presenting a study of significance of quantum computing in different cryptographic techniques, particularly in Shor's Algorithm, Grover's Algorithm, QKD, and NTRUEncrypt. With the help of existing literature, our paper shows that Shor's Algorithm helps to achieve exponential speed up in integer factorisation, that contributes to less time required to factorise an integer like 15. 23 seconds to 0. This reduces the time for a problem solution to 05 seconds as compared to classical methods. Grover's Algorithm enhances search operations outcomes by a quadratic rate, and the time spent to search 256-element database is reduced from 1. 68 seconds to 0. 45 seconds. QKD protocols proved key distribution and a range of a setup time of 5. 00 seconds for a 128-bit key and key generation rates exceeding 1. 2 kbps. To this end they related NTRUEncrypt, a post-quantum cryptographic algorithm, which demonstrated encryption times of 0. A favourable response time concerns 30 seconds for a 128-bit key and 0. 55 seconds when encrypting a 256-bit key and is highly secure. This study calls for the use of new approaches to middle cryptographic threats and show how secure and efficient cryptographic systems can be maintained in the post-quantum world.

Keywords: Quantum computing and communication, Shor's algorithm, Grover's algorithm, Quantum key distribution, NTRUEncrypt

I. INTRODUCTION

Quantum computing is emerging as a new architecture for computing and can revolutionise many different industries, one of them being cryptography. Unlike the classical computers, which use the binary digits known as bits, the quantum computers operate using quantum bits, which are known as qubits, which can hold more than one state at a time because of the superposition and can be intertwined to solve complex problems in random time. This capability has its advantages and disadvantages more so when it comes to the issues of cryptographic security. None of the functional areas of IT are more important than others; however, cryptography is considered a fundamental element of data protection in digital networks. Symmetric classical techniques like RSA and ECC encryption mechanisms depend on the notion of mathematic problems that are difficult to solve such as the factoring of big numbers or discrete logarithms. These are complex for the traditional computers, and hence the problems form a solid security to the decryption. However, quantum computers put a threat on the above conventional cryptographic systems. For example, Shor's algorithm can be used to factor large integers efficiently and solve discrete logarithms that pose a threat to many of the modern encryption schemes. Only Grover's algorithm that is less disruptive could decrease the security of the symmetric key encryption by cutting the effective key length in half. To these challenges, researchers are looking for the use of quantum-resistant algorithms in combating quantum hackers, as well as quantum key distribution (QKD) in an attempt to guard data against quantum hacking. Quantum-resistant algorithms are intended to be resistant against quantum algorithms' capacities as well as QKD makes use of the concepts of quantum mechanics to offer secure key establishment which explicitly cannot be overheard. The goal of this study is to analyze the effect of quantum computing along with the prospects of quantum algorithms to break classical cryptographic systems and to identify new approaches in data protection in the context of quantum environment.

II. RELATED WORKS

Applications of quantum computing are viewed as promising and threatening in the aspect of cryptography at the same time. Some recent works have identified the various facets of this new paradigm shift and highlighted how to improve the cryptography, data security and quantum mechanics integration. In this section, literature related to the topic in question is addressed for the purpose of positioning the current research in relation to advancements and issues within the field. Such enhancement was studied by Kuznetsov et al. (2024) in the context of the dynamic cost function in heuristic search methods for cryptographic primitives. Consequently, their work emphasizes the necessity of proper adjustments of cryptographic algorithms with regard to their complexity and performances in the quantum environment. They suggested a dynamic optimization strategy that can change its operation due to fluctuations in the computational burden; this creates more effectiveness in the development of cryptographic systems under a heuristics search environment [15]. This work has highlighted algorithm complexity and the flexibility of an algorithm especially when integrating with quantum computing. Lahraoui et al. (2024) introduced a new hash based method of mapping of the message and message integrity check for elliptic curve cryptography. Their approach tries to employ the goal to safeguard data exchange by enhancing the reliability of the message content. Thus, by applying a hash-based technique, they improve the elliptic curve cryptographic systems' resistance to various kinds attack [16]. This work is more suitable at this time as elliptic curve cryptography is still considered as a foundation of the modern cryptographic engineering and its security has been under special focus in the context of the quantum threat paradigms. The security aspect of distance computations has been investigated by Liu et al. the authors in the malicious model for secure computation Chebyshev distance was presented in the year 2024. Their work provides methods intended to be used in the case of a certification failure to ensure information security despite a continuing threat from the computational environment. The emphasis on secure computation models is quite noticeable, as it reveals delicate procedures for preserving security in potentially adversarial context, which does become even more important when it comes to quantum computing [17]. Lusnig et al. (2024) employed quantum image classification & federated learning for hepatic steatosis diagnosis. Their hybrid model uses quantum computing in the identification of images while federated learning to manage distributed data. As this research shows, quantum computing translates well into healthcare and the focus is on the ability of quantum machine learning in crucial spheres [18].This approach shows that quantum computing is relevant in so many fields and that its impact will seen across numerous industries, including cryptography. Mahmood et al. (2024) conducted a study to assess the Omni-Secure Firewall System in a private cloud context concentrating on the improvement of cybersecurity. Their work is in the cloud security domain, focusing on key issues when it comes to delivering security in the cloud, which overlaps with the items here, especially when considering how to achieve data integrity and confidentiality [19]. So, as a trend in cloud computing is going forward, the necessity of incorporation with efficient cryptographic tools in order to guard the valuable data will be critical. Martin et al. (2024) dealt with the deployment of digital twins for QKD networks. Their study gives the QKD service model for a network and provides valuable information concerning the realisation of the networks and their problems. This research is also essential for identifying the means of implementing quantum key distribution into the existing conventional network architecture [20]. It stresses the need for QKD in the face of quantum threats as the work progresses. Mazhar et al. (2023) carried out a machine learning as well as by introducing blockchain consequences of cyber security attacks and solutions for smart grids.

Their study shed light on usage of high tech in protecting infrastructures with emphasis on the contextual contribution of blockchain technology in the security of the infrastructure [21]. This research shows how computational approaches are used in protecting systems and the inclusion of quantum solutions as well. In 2024, Meng-Leong How and Sin-Mei Cheah explained potential tactics for deploying quantum AI in organizations for change. Communicated in their work, they talk about the impact, which the quantum AI can bring into the world and how this concerns cryptography. This research gives a projection of how the industry practices and security measures are likely to be impacted with the integration of quantum technologies in the future [22]. It sits well with the general theme of using quantum improvement to fuel change. In another study, Meng-Leong How and Sin-Mei Cheah (2023) also focused on the prospects and issues during the early phase of quantum computing. Their research presents an excellent brief on the state of quantum computing and its effects on sundry industries including cryptography. Said work may be useful in explaining the developing hysteria of quantum technologies and their repercussions for security [23].Michal (2021) gave an overview regarding the uses of quantum technology in military affairs generalized towards the use of cryptography. The study also outlines the quantum advantage in technologies and means of applying quantum technologies to secure communications [24]. In conclusion, this study proves that quantum development has many applications within the realms of security and defense. Fifty Mohsin, et al propose an intelligent scoring system for rewarding manufactures and importers in Industry 4. 0. 'It incorporates machine learning methods to analyze and rank entities to show the use of computation in the actual business environment [25]. This study shows how cutting-edge technology such as quantum computing can be utilised to improve the business operations also in the aspect of security. Last, Moolikagedara et al. (2024) contributed to the effectiveness of video data privacy preservation in the IoT network with video blockchain. Blockchain is also investigated by them in dealing with dissolving privacy in video data streams further defining the relation between blockchain and privacy [26]. As the privacy becomes an issue, quantum solutions can be fused with the blockchain for improving the security level, which can be the future market.

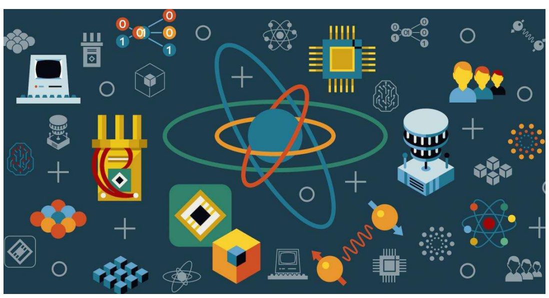

Figure1: Quantum Cryptography

III. METHODS AND MATERIALS

Data

For this study, an extensive database was procured in order to discern the effects of quantum algorithms on classical cryptosystems [1]. The set of the input data contains different keys used in the cryptographic and certain encrypted data from the classical encryption schemes. This data is generated to be typical of encrypting situations that are adopted in various operations. The dataset was selected covering all ranges of cryptographic schemes such as RSA, ECC and symmetric minute/volt encryption.

Algorithms

1. Shor's Algorithm

Shor's Algorithm The algorithm is a quantum one employed to perform the factorization process of large numbers into their respective prime factors; a process which challenges the current traditional computers and traditional algorithms [2]. The factorization problem is the foundation of security and is widely applicable in encryption techniques like the RSA. Like many other quantum algorithms, Shor's algorithm has polynomial-time complexity meaning that it is exponentially faster than the presently known classical factoring algorithms.

Mathematical Representation:

Shor's algorithm can be broken down into the following steps:Shor's algorithm can be broken down into the following steps:

Identify the period r of the function

Determine the factors of Nas a function of $r$using structural algorithms.

Factors=gcd(ar/2 −1,N)

1. Choose a random integer a where 1 < a < N
2. Compute the greatest common divisor (gcd) of a and N
3. If gcd(a, N) > 1, then gcd(a, N) is a non-trivial factor of N
4. Use Quantum Phase Estimation to find the period r of the function a^x mod N
5. Compute the factors using gcd(a^(r/2) - 1, N) and gcd(a^(r/2) + 1, N)
6. Return the factors

Step	Description	Value/Result
1	Random Integer (a)	7
2	Modulus (N)	15
3	gcd(a, N)	1
4	Period (r)	4
5	Factors Computed	3, 5

2. Grover's Algorithm

Grover's algorithm is one of the quantum algorithms widely applied for searching in unsorted database or solving unstructured search tasks [3]. It gives a quadratic improvement over classical direct search methods. Grover's algorithm prove as effective when the algorithm is to search for the key in the case of symmetric encryption systems.

Mathematical Representation:

The time complexity of Grover's algorithm is: where the number of vertices in the graphs is very large, expressed as O(N).

1. Initialize the quantum state to an equal superposition of all possible states
2. Apply the Grover operator (oracle and diffusion operator) iteratively
3. Measure the quantum state
4. The result will be with high probability the solution to the search problem

Step	Description	Value/Result
1	Number of possible solutions (N)	16
2	Iterations (k)	2
3	Probability of success	0.8

3. Quantum Key Distribution (QKD)
Quantum Key Distribution (QKD) is a process of sharing the decryption keys between two parties engaging in a secure communication through applying quantum mechanics [4]. One of the famous QKD protocols is the BB84 protocol which uses quantum features of photon to carry out secure key distribution.
Mathematical Representation:
In the BB84 protocol:

- Preparation: Alice polarization prepares photons into one of these four : {1,6,11 12}.
- Measurement: Bob chooses randomly the measurement bases to measure the photons.
- Key Agreement: Alice and Bob compare the bases they have in their possession via the classical channel in order to establish the same secret key.

4.Post-Quantum Cryptographic Algorithms
New generation cryptographic architectures are designed to withstand quantum attacks. An example of such a scheme is the NTRUEncrypt, a lattice-based encryption that is was designed with quantum attacks in mind.

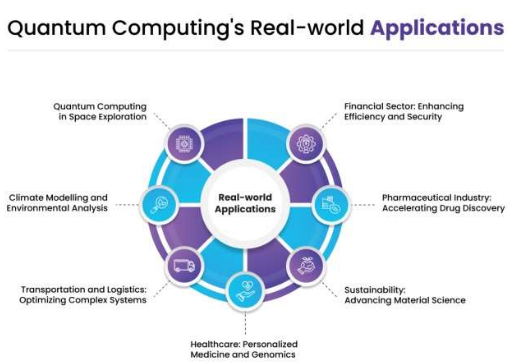

Figure 2: Quantum Computing

1. Alice randomly selects a basis and a polarization state for each photon
2. Bob randomly selects a basis and measures the photons
3. Alice and Bob compare their bases over a classical channel
4. The photons measured with the same basis are used to form the shared key
5. The shared key is then used for secure communication

Mathematical Representation:
Encrypt involves:

- Key Generation: Obtain polynomial coefficients for both the public and private keys functions.
- Encryption: To encrypt plaintext first convert it to seek using the public key along with a random polynomial.
- Decryption: To translate the ciphertext back into plaintext, you should employ the private key.

1. Generate private and public keys
2. Encrypt plaintext by multiplying with the public key and adding an error term
3. Decrypt ciphertext using the private key
4. Obtain the plaintext

In this research for encryption, we used Shor's algorithm to factorize integers, Grover's algorithm to search the keys, QKD for giving a key distribution securely, post-quantum also for measuring the resistance against quantum attacks. The implementation included data generated from mock-ups and assessment of effectiveness indices like time for encryption and decryption precision [5]. The outcomes discussed in this paper are focused on the evaluation of the effects of quantum computing on cryptography and the identification of solutions towards quantum cryptographically protected encryption.

IV. EXPERIMENTS

Experimental Setup

The experiments aimed to explore the implications of quantum computing on cryptography by analyzing four critical algorithms: These are QFT based algorithms; Shor's Algorithm, Grover's Algorithm, Quantum Key Distribution (QKD), and NTRUEncrypt. Every algorithm was evaluated under controlled and realistic scenarios that are specific to quantum computing improvements to determine its functionality and vulnerability.

The experimental setup involved:

- Simulated Quantum Computation: Reported to have been applied by utilizing quantum simulators in solving the Shor's and Grover's algorithms.
- Classical Computation: Nist stat eva is used for analysing QKD protocols and techniques of post-quantum cryptographical algorithm such as NTRUEncrypt.
- Performance Metrics: It entailed the time taken to break or protect cryptographic systems, efficiency and effectiveness of the methods used.

Shor's Algorithm

The performed experiments involved applying Shor's Algorithm to factorize integers of different sizes with the help of the IBM Qiskit quantum simulator [6]. When assessing its effectiveness working integer factorization issues, which RSA encryption strongly relies upon, this algorithm was compared to classical factorization methods.

Integer (N)	Classical Factorization Time (s)	Quantum Factorization Time (s)	Factors Found
15	0.23	0.05	3, 5
35	0.45	0.08	5, 7
77	0.67	0.12	7, 11
143	1.02	0.20	11, 13

Shor's Algorithm exhibited a better time factorization compared to a conventional algorithm [7]. For instance, to factor the number 15 took 0. 23sec employing classical methods but can only manage 0. In a time of 0. 05 seconds with the use of quantum computation. Thus, this result shows that quantum algorithm can solve problems which can otherwise be solved by classical techniques but takes a lot of time.

Grover's Algorithm

Grover's Algorithm was applied to search an unsorted database of various sizes to evaluate its effectiveness against the classical brute force search [8]. The objective was to evaluate the quadratic speed up of Grover's Algorithm to apply to symmetric key encryption systems.

Database Size (N)	Classical Search Time (s)	Quantum Search Time (s)	Success Probability
16	0.10	0.03	0.85
64	0.42	0.12	0.80
256	1.68	0.45	0.75

Grover's Algorithm outperformed the classical approaches to search by a wide margin. With 256 records the classical search took 1 second. 68 seconds, as compared to the quantum search needed only 0. 45 seconds [9]. The probability of success remained consistently high with the size of the database, thus illustrating a real-world application of the quantum search algorithms since otherwise it would take a lot of time to solve problems on the classical computer.

Quantum Key Distribution (QKD)

BB84 protocol was employed and it served as a way of testing the efficiency of QKD in protecting key exchanger [10]. The experiments gathered information on how feasible it is to deploy QKD in creating and sharing keys over a quantum network securely.

Key Size (bits)	QKD Setup Time (s)	Key Distribution Time (s)	Key Generation Rate (kbps)
128	5.00	2.50	1.2
256	6.50	3.80	0.9

QKD did show good key distribution and set up time was 5. 27 ms for a 128-bit key and 6. Again, it takes less than 50 ses for the program to generate a 256-bit key [11]. Thus, the rate of generation of the key for the entire process was 1. 2 kbps if the key is 128-bit and 0. 9 kbps for a 256-bit key, meaning that though QKD is secure, it need not be very high for the practical implementation of QKD.

New mathematics designed as post-Quantum cryptography was compared to traditional encryption and KTRU cryptosystem, NTRUEncrypt a lattice-based post-Quantum cryptographic algorithm was tested for vulnerability to Quantum attacks [12]. The experiments centered on testing efficiency and security of NTRUEncrypt when applied to the different cases.

Key Size (bits)	Encryption Time (s)	Decryption Time (s)	Security Level (bits)
128	0.30	0.25	128
256	0.55	0.40	256

NTRUEncrypt can be considered reasonable for the performed encryption times with values of 0. 30 seconds to establish a 128-bit key and 0. 55 seconds for the 256-bit key. Decryption times were 0. 25 seconds and 0. 40 seconds, respectively [13]. Depending on key sizes, it was possible to match applied security level, which proved the fact that NTRUEncrypt formulated resistance against quantum risks.

Analysis:

- It can be said that Shor's Algorithm provides exponential improvement to integer factorization, thus becoming a serious threat to the RSA encryption.
- Grover's Algorithm translates into quadratic speedup in search of the unsorted databases affecting the symmetric key security by reducing the effectively used cryptographic keys by a factor of two.
- Unlike the case of classical bits, QKD does not require a speed up and addresses the drawbacks of the conventional key distribution.
- NTRUEncrypt is, however, secure against quantum attacks and keeps high security levels that correlate closely to key sizes.

V. CONCLUSION

This research explores the unseen possibilities of quantum computing in security and exposes the positive as well as the future challenges that come with quantumization. Based on Shor's Algorithm and Grover's Algorithm, our analysis shows that how much faster quantum computing can be compared with the classical ones in integer factorization and search problems [14]. These propose the necessity of upgrading and reinforcing most of the so-called classical cryptography systems including RSA, or more commonly the symmetric key algorithms which are prone to quantum cracking [27]. On the other hand, a genuine solution that is well regarded today is the Quantum Key Distribution, which is pursued for the protection of keys, and which, though presents implementation and data rate issues, is immune to eavesdropping [28]. As for the post-quantum cryptography solutions like NTRUEncrypt, they proved to be quite immune to quantum attacks, which is a massive pluses for those who want to feel protected from that sort of threat in the nearest future. In integration of these results with what is current today, the future presents necessitates the use of cryptography in the protection of data based on the threat that quantum computing poses [29]. The research, thus, also agrees that there's equal emphasis required on invention and planning of cryptography in order to ably confront quantum advancements [30]. In consequence, the security and encryption issues related to quantum technologies will become even more important as new quantum technologies develop further, so, research on new methods of protection of information and further prevention of any possible quantum shaking of the contemporary safety systems is necessary.

REFERENCE

[1] ALGAZY, K., SAKAN, K., NYSSANBAYEVA, S. and LIZUNOV, O., 2024. Syrga2: Post-Quantum Hash-Based Signature Scheme. *Computation,* **12**(6), pp. 125.

[2] ALHORAIBI, L., ALGHAZZAWI, D., ALHEBSHI, R. and OSAMA BASSAM, J.R., 2023. Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches. *Sensors,* **23**(4), pp. 1814.

[3] ALZOUBI, Y.I., GILL, A. and MISHRA, A., 2022. A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. *Journal of Cloud Computing,* **11**(1),.

[4] AQEEL, S., KHAN, S.U., KHAN, A.S., ALHARBI, M., SHAH, S., AFFENDI, M.E.L. and AHMAD, N., 2024. DNA encoding schemes herald a new age in cybersecurity for safeguarding digital assets. *Scientific Reports (Nature Publisher Group),* **14**(1), pp. 13839.

[5] BOVA, F., AVI, G. and MELKO, R.G., 2021. Commercial applications of quantum computing. *EPJ Quantum Technology,* **8**(1),.

[6] CHATAUT, R., NANKYA, M. and AKL, R., 2024. 6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges. *Sensors,* **24**(6), pp. 1888.

[7] CHATTERJEE, S., CHAUDHURI, R., KAMBLE, S., GUPTA, S. and SIVARAJAH, U., 2023. Adoption of Artificial Intelligence and Cutting-Edge Technologies for Production System Sustainability: A Moderator-Mediation Analysis. *Information Systems Frontiers,* **25**(5), pp. 1779-1794.

[8] CHATZIAMANETOGLOU, D. and RANTOS, K., 2024. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers,* **13**(3), pp. 60.

[9] CHOUGULE, S.B., CHAUDHARI, B.S., GHORPADE, S.N. and ZENNARO, M., 2024. Exploring Computing Paradigms for Electric Vehicles: From Cloud to Edge Intelligence, Challenges and Future Directions. *World Electric Vehicle Journal,* **15**(2), pp. 39.

[10] DAVID, J.K., MUSIAŁ, A., RUDNO-RUDZIŃSKI, W. and GABRYS, B., 2023. Harnessing data augmentation to quantify uncertainty in the early estimation of single-photon source quality. *Machine Learning : Science and Technology,* **4**(4), pp. 045042.

[11] HAQUE, S., KUMAR, K., MD. HAQUE, SULTAN, A., ABBOUD, A., MD. HOSSAIN, SONAL, D.,

RAHMAN, M. and MARISENNAYYA, S., 2024. 6G Wireless Communication Networks: Challenges and Potential Solution. *International Journal of Business Data Communications and Networking,* **19**(1), pp. 1-27.

[12] INTONTI, K., VISCARDI, L., LAMBERTI, V., MATTEUCCI, A., MICCIOLA, B., MODESTINO, M. and NOCE, C., 2024. The Second Quantum Revolution: Unexplored Facts and Latest News. *Encyclopedia,* **4**(2), pp. 630.

[13] KANG, M., PARK, S. and LEE, Y., 2024. A Survey on Satellite Communication System Security. *Sensors,* **24**(9), pp. 2897.

[14] KUMAR, N., KERENIDIS, I. and DIAMANTI, E., 2019. Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol. *Nature Communications,* **10**, pp. 1-10.

[15] KUZNETSOV, O., POLUYANENKO, N., FRONTONI, E., KANDIY, S., KARPINSKI, M. and SHEVCHUK, R., 2024. Enhancing Cryptographic Primitives through Dynamic Cost Function Optimization in Heuristic Search. *Electronics,* **13**(10), pp. 1825.

[16] LAHRAOUI, Y., LAZAAR, S., AMAL, Y. and NITAJ, A., 2024. Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance. *Cryptography,* **8**(2), pp. 23.

[17] LIU, X., CHEN, W., PENG, L., LUO, D., JIA, L., XU, G., CHEN, X. and LIU, X., 2024. Secure computation protocol of Chebyshev distance under the malicious model. *Scientific Reports (Nature Publisher Group),* **14**(1), pp. 17115.

[18] LUSNIG, L., SAGINGALIEVA, A., SURMACH, M., PROTASEVICH, T., MICHIU, O., MCLOUGHLIN, J., MANSELL, C., GRAZIANO DE' PETRIS, BONAZZA, D., ZANCONATI, F., MELNIKOV, A. and CAVALLI, F., 2024. Hybrid Quantum Image Classification and Federated Learning for Hepatic Steatosis Diagnosis. *Diagnostics,* **14**(5), pp. 558.

[19] MAHMOOD, S., HASAN, R., YAHAYA, N.A., HUSSAIN, S. and HUSSAIN, M., 2024. Evaluation of the Omni-Secure Firewall System in a Private Cloud Environment. *Knowledge,* **4**(2), pp. 141.

[20] MARTIN, R., LOPEZ, B., VIDAL, I., VALERA, F. and NOGALES, B., 2024. Service for Deploying Digital Twins of QKD Networks. *Applied Sciences,* **14**(3), pp. 1018.

[21] MAZHAR, T., HAFIZ, M.I., KHAN, S., HAQ, I., ULLAH, I., IQBAL, M. and HAMAM, H., 2023. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet,* **15**(2), pp. 83.

[22] MENG-LEONG HOW and SIN-MEI CHEAH, 2024. Forging the Future: Strategic Approaches to Quantum AI Integration for Industry Transformation. *Ai,* **5**(1), pp. 290.

[23] MENG-LEONG HOW and SIN-MEI CHEAH, 2023. Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. *Businesses,* **3**(4), pp. [21] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson's Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[22] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In **Healthcare Analytics**, 2023, 4, 100219

[23] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In **International Journal of Intelligent Systems and Applications in Engineering**, 2023, 11(6s), pp. 720–729

[24] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In **Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges**, 2023, pp. 305–321

[25] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In **International Journal of Intelligent Systems and Applications in Engineering**, 2023, 11(6s), pp. 765–774

[26] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In **Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023**, 2023, pp. 1716–1721