2022 Fourth International Conference on Advanced Science and Engineering (4th ICOASE)
University of Zakho - Duhok Polytechnic University - Northern Technical University, Kurdistan Region, Iraq

Influence of Quantum Computing on IoT Using Modern Algorithms

Zainab Salih Ageed
Computer Science Dept.,
Nawroz University
Duhok, Iraq
zainab.ageed@nawroz.edu.krd

Subhi R. M. Zeebaree
Energy Eng. Dept.,
Duhok Polytechnic University
Duhok, Iraq
subhi.rafeeq@dpu.edu.krd

Rezgar Hasan Saeed
Information Technology Dept.,
Duhok Private Technical Institute
Duhok, Iraq
rezgarhasan1992@gmail.com

2022 4th International Conference on Advanced Science and Engineering (ICOASE) | 978-1-6654-7222-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICOASE56293.2022.10075583

***Abstract*— Even while the Internet of Things (IoT) already affects our day-to-day activities, its future relevance and potential for transformation remain untapped. Security issues with present communications technology must be solved before secure end-to-end connection between services can be achieved. Internet of Things (IoT) is here to stay. In the next years, it will become an integral part of our everyday life. There is a good chance that sensor-based networks can recognize it as a direct service provider in our surroundings. Even if it's just in the form of a value-added service delivered through cellular networks, it's going to be helpful nevertheless. It is, nevertheless, subject to a wide range of security threats. The current level of security is insufficient for IoT applications in the future. A secure cryptosystem is needed for the Internet of Things. quantum-based security has seen a surge of attention recently. Additional quantum key distribution systems and network services are now supported by this solution. As a result of the quantum computing's unrivaled security level, it has become more popular in recent years. Because every measurement must affect the state of the quantum bit being sent, quantum physics dictates that this must be the case. Regardless of whether the sender or recipient is aware of the change, it is clear. It is thus no longer possible to listen passively. Polarized photons may encode a string of bits using protocols like BB84. Secure cryptographic keys may be generated over an unsafe channel utilizing various key distillation procedures.**

Keywords*— *Quantum Computing, IoT, Security, Communication.

I. INTRODUCTION

People building intelligent machines using Semantic. The current communication technologies have several security concerns that must be addressed to provide safe end-to-end connectivity between services. Furthermore, most standard security measures deemed secure may be jeopardized due to the recent, rapid rise of quantum technology [1]. As a result, to withstand various possible quantum computer assaults, current security mechanisms require quantum technologies during their development [2]. The Internet of Things (IoT) has become an increasingly important component of the future. The IoT has become an increasingly important component of the future [3] [4]. The Internet of Things (IoT) is a network like the Internet that connects a large number of items. These items are made up of a combination of electronics, sensors, and software that controls how the object's other pieces operate. Each thing uses sensors to create and gather data from its surroundings, which it then sends to other objects or a central database via a channel [5, 6]. Multiple users wishing to originate or send a shared quantum-secured communication are the subject of ongoing research in quantum communications networks. To allow the next generation of quantum communication networking and simultaneously address the issues with discrete variable- and continuous variable-quantum key distribution technique[8, 9].

In order to implement the distribution of keys with verifiable security, also known as quantum key distribution (QKD), quantum communication (QuCom) uses quantum information theory concepts, in particular the no-cloning theorem and the theorem of indistinguishability of arbitrary quantum states. With QKD, security is guaranteed by the fundamental laws of physics as opposed to unproven mathematical assumptions used in computational security-based cryptography [4]. It promises a vast web of "things" that connects everything, everyone, everywhere, at all times, and across all networks. Devices, sensors, services, apps, and other intelligent nodes will connect and communicate in real-time under this idea [12-14]. Due to the presence of internet technology, which confirms shifts in market patterns, human activities, communication, transport, factories, etc., several industries that are deemed disruptive and threaten different sectors have been included in the IoT study [7, 10]. It promises a vast web of "things" that connects everything, everyone, everywhere, at all times, and across all networks. Devices, sensors, services, apps, and other intelligent nodes will connect and communicate in real-time under this idea. Web-enabled data exchange will usher in IoT, which will improve service delivery and connect devices. Furthermore, the Internet of Things (IoT) will serve as a platform for bringing the physical and virtual worlds together [11, 15, 16].

Quantum computing make viral diffusion simulations feasible for large networks, independent of network topology [17]. Quantum-based security is a novel communication network end-user security solution. Despite the fact that many notions (such as super-dense coding or quantum teleportation) are comparable, quantum cryptography (QC) is the first implemented idea for communications networks. Numerous

978-1-6654-7222-7/22/$31.00 ©2022 IEEE

technological issues must be addressed before it can be extensively utilized [18]. Because of issues with quantum signal regeneration, quantum communication across vast distances is currently a significant concern. Modern amplifiers directly impact quantum bits, changing the information conveyed. Currently, the maximum length covered by successful QKD broadcasts exceeds 200 kilometers. In a distinctive telecom MAN, the bit rate of QKD systems is a few Mbit/s. Even QKD between the Earth and retroreflector-equipped LEO satellites is feasible. Until recently, banks, large companies, and government agencies were the most likely end users of QKD methods. The expense of QC technology is one of the reasons why only big companies can afford to use it. Quantum devices to broadcast and receive quantum bits, as well as additional optical fiber to form a quantum channel, are two aspects that add up to a significant cost.

The new network, which includes 2000 kilometers of optical fiber with eighty quantum cryptography units, price around $2,000,000. Only prominent players can justify such a high expense, then long-standing asset considered as advantageous if the status or reputation it provides been considered [9, 19]. Quantum technologies offer the highest level of data security. End-users can access quantum cryptography services and devices. But a wondering still remained: how can users manage and control the security provided with those explanations? Regardless are current network facilities care QKD, operators cannot tailor facility to their specific requirements. As a result, users should evaluate the level of security offered by quantum-based systems and choose the appropriate level of data security [20]. Quantum technologies provide the highest level of data security. Quantum cryptography services and equipment are available to end consumers. But there's another question: What are the options for users to manage and regulate the security offered by these solutions? Even though current network services enable QKD, users are unable to customize the service to their unique requirements. As a result, users should evaluate the level of security offered by quantum-based systems and choose the appropriate level of data security [21] . The transformation of understandable data into an unrecognizable form is referred to as data encryption. Digital pictures are a type of data representation that is widely utilized in a variety of applications [22].

II. BACKGROUND THEORY

A. Quantum Computing

Quantum computing is a brand-new field that uses quantum physics to do calculations. Mathematics, physics, and computer science are all included in this project. In the 1980s, scientists pondered if a universal machine might mimic quantum mechanical systems [14]. Although, the current quantum computers, their practical use is minimal. The topic takes tremendous promise, however studies are till now ongoing, the future cannot be predicted. Could anybody have foreseen widespread internet usage everyday lives in the 1990s. Quantum computing, on the other hand, is still in its infancy. Because existing quantum circuits are vulnerable to noise, researchers have dubbed this period the noisy intermediate-scale quantum (NISQ) era. It is hoped that devices in the NISQ era would soon begin to demonstrate practical applications in optimization, machine learning, cryptography, finance, and quantum mechanical system modelling [13, 23, 24]. In the field of quantum computing, there are two major challenges. The first step is to make sure the experimental quantum processor has enough good qubits. Contemporary computer qubit technologies include ion traps, Majorana, semiconducting and superconducting qubits, NV-centers, and even graphene. It's difficult to improve the overall state of the qubits since they suffer from de-coherence, which causes mistakes while conducting quantum gate operations.

The quantum accelerator will only become a widely used solution where diverse quantum technologies are shown on the lowest layer if the quantum physical community overcomes those problems. This direction is shown in the left picture of Fig. 1. The second challenge is articulating the quantum logic that companies and other organizations require when using high-performance accelerators for specialized computations that can only be performed at a high level on a quantum device. Companies who wish to pursue this path and reap the advantages will need to make a long-term commitment to personnel and technological know-how. The industry's promise to examine the needed quantum logic, which can be built using the entire stack and evaluated and validated using a quantum simulator, is shown in the right section of Fig. 1. It's important to note that the qubits are referred to as "perfect qubits" since they don't de-cohere or make any other errors. With the introduction of vast amounts of data, nicknamed "big data," it's become evident that this methodology isn't scalable to extremely large data sets. The main cause is the enormous amount of data that needs to be processed over several computer cores, which is a tough task [25].

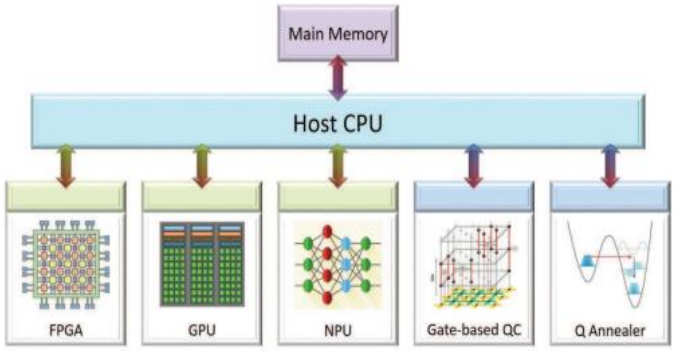

Fig. 1. System architecture with heterogeneous accelerators [26].

B. Principles of Quantum

A qubit, the quantum counterpart of a conventional bit, is the quantum information unit (quantum bit). Qubits, like bits, can have two possible values or a combination of the two. A quantum item can exist in a superposition state before being measured; nevertheless, the measurement may cause this state to be damaged. After that, the measurement will be used to ascertain the object's condition. One of quantum mechanics' essential concepts was published by Werner Heisenberg in 1927. He demonstrated that the location and momentum of a physical system cannot be assigned precise instantaneous values and that these variables can only be calculated with a

certain amount of uncertainty. The Heisenberg uncertainty principle asserts that measuring physical quantities with the same high accuracy is impossible. One example of such a pair is position and momentum. Polarizations of photons are another example [27, 28]. Quantum computers with up to 50 qubits have been constructed, with the goal of extending this to 100 qubits by 2020. Quantum computers have been developed by large corporations such as Google, IBM, and Microsoft, as well as startups like as Rigetti, D-Wave, and Xanadu. IBM has built a quantum computer. Thanks to a software development kit (SDK) produced by organizations, the general public may also experiment with quantum computers. Users may also use cloud-based services to run their applications on a genuine quantum computer. Two examples of such services are Rigetti Forest and IBM Quantum Experience [29, 30].

III. Related Work

[2] Presented a security and storage performance algorithm. The quantity of information rises as of 200 towards six hundreds, without information losing by any 3 ways, showing their storing bulk practically similar. With transferred information quantity exceeding 800, however, HDFS storing and spread storing techniques experience noticeable data loss, cumulative information volume communicated. On the other hand, the described approach didn't suffer from data-losing through all stages, showing capability of preserving data truthfulness with enormous amounts of data.

[3] Introduced a flexible and broad cumulative distribution table (CDT)-based Gaussian sampler using a hardware-software method. An AHB interface is included in the planned CDT sampler. It may be configured to handle a wide range of parameter setups with only 77 slices on a Xilinx Spartan-6 FPGA and a consistent response time. This study identifies the vulnerability associated with three fundamental procedures in any binary search state. With just an extra 58.4 percent Slices, an effective countermeasure based on randomness may be built.

[9] Proposed design performs better with the fewest gates and low time complexity. They used systolic architectures to multivariate cryptographic systems to compute inversions in finite fields. The suggested architecture satisfies IoT supply necessities besides the protected data management requirements of modern manufacturing. The suggested architecture is more performant and fulfils the resource requirements of IoTs and the secure data management requirements of advanced manufacturing, making it ideal for developing different cryptographic systems.

[10] Suggested a worldwide quantum network of satellites to offer coverage. Quantum subnetworks of LEO satellites will comprise the quantum satellite network. An MEO satellite subnetwork will connect certain quantum subnetworks based on LEO satellites. Subnetworks of MEO satellites will be linked to the global GEO satellite network in the future. Terrestrial quantum networks will be linked using LEO/MEO satellites. Each quantum communication subnetwork will use the cluster state idea. It will construct EPR pairings for two nodes in the global network using a global quantum network.

[12] Looked at the current and future uses of quantum computing. Based on quantum computing, Grover's method does not employ any internal structure of the supplied function f, even if it has one. The algorithm's or oracle is f. This approach has a temporal complexity of a quadratic factor faster than traditional computational models. The oracle causes the amplitude of the designated state to become negative, and then that state is amplified. The amplitude of the target state is maximized after an adequate number of repetitions.

[13] Suggested a generic quantum approach for open quantum dynamics evolution and proven on quantum computing devices. The Sz.Nagy theorem guarantees that time-controlling Kraus operators may be turned into unitary matrices with minimal dilation. Hence, leads to permits unitary quantum gates to build the initial state while requiring significantly less energy than standard Stinespring dilation. Despite their importance in representing the system-environment interaction seen in most real-world physical models, quantum algorithms for open quantum dynamics have made tremendous progress.

[16] Examined the system by using Maurer and Renner's Constructive Cryptography methodology. First, identify RSPCC's aim to create optimal RSP resources from traditional channels, exposing RSPCC's security constraints. A crucial link between the work of cloning quantum states and the challenge of building optimal RSP resources (from classical channels) was discovered. Even if just caring about computational security, every classically built ideal RSP resource must leak the entire classical description (perhaps in an encoded form) of the produced quantum state to the server.

[17] Created nonlinear dynamical systems to forecast dissemination across networks (NLDSs). These models, particularly for networks with static topologies, provide good approximations of real-world dispersion. The computing cost of simulating viral propagation, on the other hand, makes it unsuitable for large-scale networks. It has been proved that quantum computing may be used to simulate viral diffusion in large networks independent of network architecture.

Simulations showing an error-free quantum circuit successfully replicated viral spread in a network with N = 5 nodes and t = 20-time steps, with multivariate Euclidean distances from expected infection probability peaking near 8%. This degree of accuracy is sufficient for distinguishing between nodes' relative susceptibilities and detecting critical transitions, such as times of extremely high susceptibility.

IV. Discussion and Recommendations

A. Discussion and Comparison

It's worth noting that the authors of [14] developed a unique cybersecurity strategy based on quantum-inspired quantum walks and QHF in their prior work. While [15], researchers examined the performance of the ECC encryption method, the RSA encryption technique, and the DSA encryption algorithm regarding data storage security. The RSA and DSA algorithms' sub-exponential time and space complexity, on the other hand, may be determined using the formula [16]. The numerical analysis of their data and the results of the simulations offered

by [17] provided enough evidence to accurately infer that the photo encryption technique is dependable and efficient in protecting patients' privacy. [18] Focused on the inversion in the proposed GF2n 2 inversion, which takes 2n2 6n, it takes two clock cycles to compute and a total of n AND gates and 4n XOR gates to complete the task. A situation in which unconnected terrestrial quantum coherence networks are linked by a low Earth orbit (LEO) satellite quantum network, resulting in a heterogeneous satellite-terrestrial quantum coherence network, as described by is described in depth in [19]. Furthermore, researchers claim that [20] made a remark about quantum algorithms that have been used as subroutines in enormous machine learning systems. [21] IBM Qiskit quantum simulator and IBM Q 5 Tenerife quantum device have been used. However, the authors discovered in [22] that achieving shared RSP resources without substantially decreasing their claims was unfeasible because of the no-cloning theorem. [23] discovered that quantum n AND gates and 4n XOR gates are used in total, taking two clock cycles to compute. A situation in which unconnected terrestrial quantum coherence networks are joined by a low Earth orbit (LEO) satellite quantum network, resulting in a heterogeneous satellite-terrestrial quantum coherence network, as described by is described in detail bys, demonstrating that quantum computing can be used in the real world. In the literature review section, Table I shows a sufficient comparison of all previously mentioned publications.

TABLE I COMPARISON AMONG MOST RELATED PREVIOUS WORKS FOR QUANTUM COMPUTING INFLUENCE ON IOT

Ref.	Algorithms	Models and Tools	Significant Outcomes
[2] 2020	Cryptographic algorithms include the DSA algorithm as well as ECC and RSA.	The DoS Both physical and virtual machine attacks were unsuccessful in getting access to the storage.	Improved algorithms have been verified for effectiveness and feasibility, enhancing IoT communication security without sacrificing user convenience. The ECC encryption algorithm is presented in this work to safeguard IoT data consists of information. Data compression based on blockchains is the focus of this research, which employs compressed sensing. to speed up data storage for information storage. The outcomes of the experiments back up the method's efficiency.
[3] 2020	A hardware-software technique is used to create a CDT-based Gaussian sampler.	AHB interface used and handled different parameter settings with only A Spartan-six FPGA with seventy-seven slices. SPA attack is as a sampler is demonstrated.	The proposed CDT sampler has several advantages, including high hardware flexibility, side-channel security, and usability for resource-constrained IoT nodes.
[9] 2020	The extended Euclidean algorithm was used to suggest a binary inversion algorithm.	Each inversion in the proposed inversion in GF2n2 requires 2n2 6n, and takes n AND gates and 4n XOR gates total clock cycles to compute.	Data management should be improved based on security measurements.
[10] 2020	Lines of (SMF) and (FMF) nodes using (DWDM).	SDN-based QCN architecture has 3 layers: QCN layer, application layer, and a network layer.	Provide unmatched security the IoT, optical networks, and 5G+/6G wireless networks self-driving automobiles.
[12] 2020	Grover's algorithm	Usaing of two quantum systems to exchange roles between iterations.	Although they may be costly to perform in practice, the suggested algorithms give a speedup. The physical manifestation of a quantum computer is also difficult for quantum algorithms.
[13] 2020	The density matrix is evolved using a quantum algorithm.	Density matrix created and physical data extracted. Each physical composition develops it with minimal Kraus operator Mk Sz.-Nagy dilations.	The suggested approach is easily generalizable to various other free quantum dynamical models; since it does not require specific quantum channel dynamics or decomposition models.
[16] 2020	Preparation of the classical-client remote state	Using the Constructive Cryptography framework as a traditional channel	The resultant UBQC protocol loses its established compostable security when RSPCCRSPCC is utilized as a subroutine. Given that the RSPCCRSPCC could be replaced by UBQCUBQC protocol.
[17] 2020	nonlinear dynamical systems (NLDSs)	In a network with 5 nodes and 20 time-steps probability, the quantum circuit properly simulated Multivariate Euclidean distances from projected infection, and= 8%.	The findings show that quantum computational network simulation can produce realistic diffusion models in vast networks, which is an actual real-world application of quantum computing. Researchers from several fields who want to understand and predict viral dissemination would benefit significantly from the capacity to mimic viral diffusion.

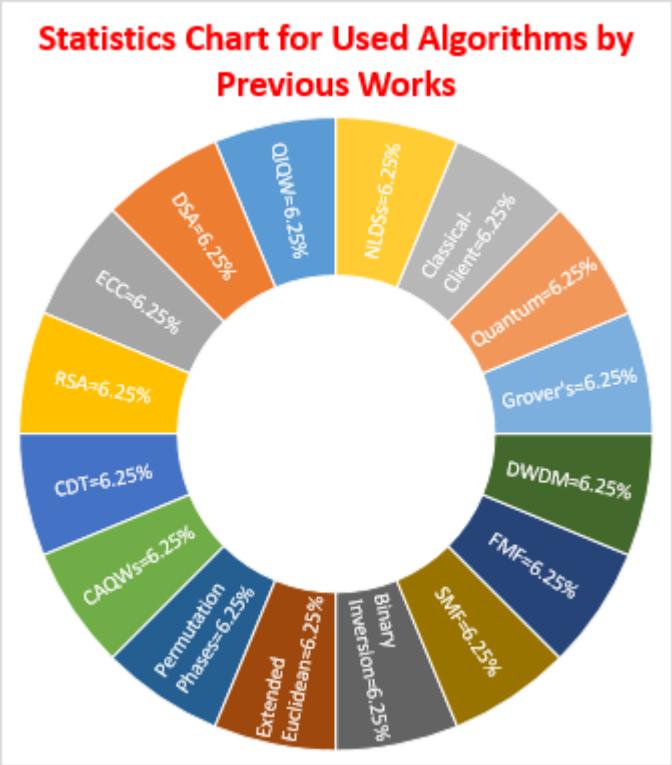

Fig.2. Statistics Chart for Used Algorithms by Previous Works.

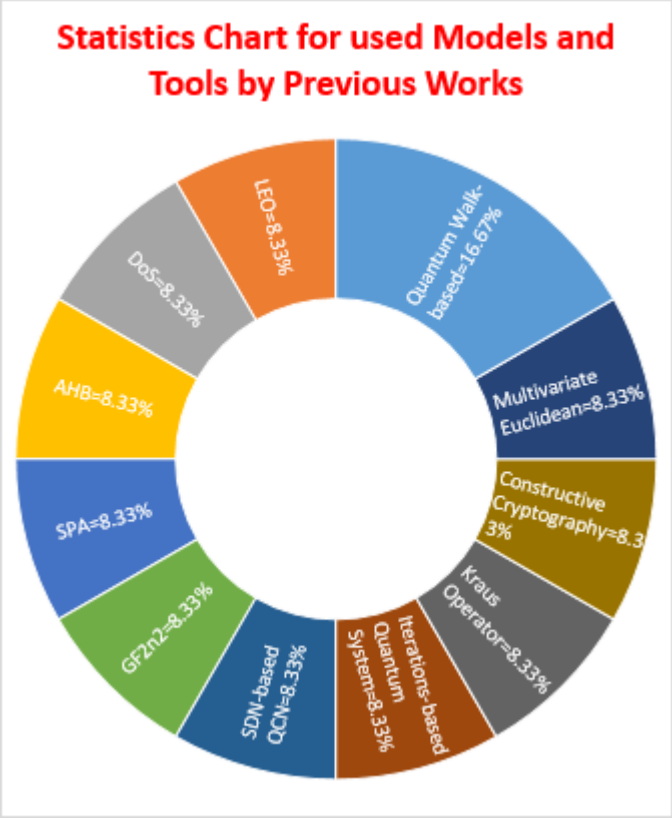

Fig.3. Statistics Chart for Used Models and Tools by Previous Works.

As statistical computations extracted from the previous, three types of statistics are computed and plotted as shown in Figs. 2, 3, and 4. The first statically computation metric is related to the previous depended algorithms, as shown in Fig. 2. It is clear that all conducted 16 different algorithms have the same percentage usage of 6.25% for each. While, the second statistical computation metric is related to models and tools used by previous works as shown in Fig. 3. There are famous 11 models and tools have been depended by the previous works. The plot shows that the Quantum Walk-based model has 16.67%, which is twice percentage usage of all remained 10 models and tools each has 8.33% usage. Finally, the significant outcomes metric of the previous works been computed and plotted as shown in Fig. 4. There are main 12 outcomes targeted by the previous works. The plot shows that 10 metrics have the same percentage usage which is 6.25% for each. And the quantum-inspired blockchain metric has 12.25% percentage usage. However, the security metric has most percentage usage which is 25%.

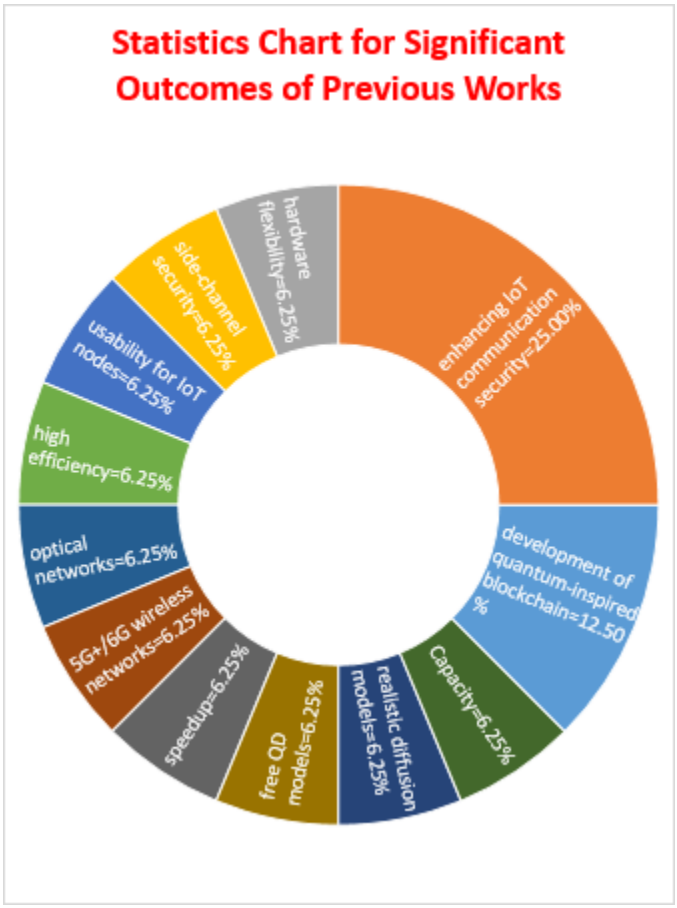

Fig.4. Statistics Chart for Significant Outcomes of Previous Works.

B. Recommendations

Several important points can be recommended from the previous works addressed in the (related work, and discussion and comparison) sections. It is recommended that the researchers take care of the security metric in their works. Also, they should depend on the quantum hash algorithms based on QIQW within their work to provide more system support. Finally, the Quantum Walk-based model provides more efficiency to the system.

V. CONCLUSION

Based on the information that is presented in Table I, it is possible to arrive at the conclusion that the application of quantum computing to the Internet of Things has developed into a very major subject and offers researchers an exciting way to carry out their research. This conclusion is reachable because of the information that is presented in Table I. The fact that it is feasible to achieve this goal lends credence to the previously stated assertion. The quantity of data that is available places limits on the breadth of the study that can be conducted as well as the number of options that may be picked. Due to the fact that healthcare systems are now one of the most significant components of our day-to-day lives, there has been an exponential rise in the quantity of medical data, which includes information on patients as well as photos of medical conditions and procedures. This is as a result of the fact that healthcare systems have evolved into one of the most critical elements of our day-to-day lives. As a result of this increase, there is now a need for a greater capacity for processing in order to ensure that this information is kept current. In order to conduct systolic inversion in composite fields, existing multivariate cryptography systems may be able to take use of resource needs that are compatible with the internet of things (IoT) and enjoy the advantages that come along with them. Wireless networks, optical networks, and self-driving vehicles have all received an additional layer of security as a direct result of recent technological breakthroughs. This is to protect them from any possible dangers that may arise.

REFERENCES

[1] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," Information Processing & Management, vol. 58, p. 102549, 2021.

[2] Y. Liu and S. Zhang, "Information security and storage of Internet of Things based on block chains," Future Generation Computer Systems, vol. 106, pp. 296-303, 2020.

[3] C. Zhang, Z. Liu, Y. Chen, J. Lu, and D. Liu, "A flexible and generic Gaussian sampler with power side-channel countermeasures for quantum-secure Internet of Things," IEEE Internet of Things Journal, vol. 7, pp. 8167-8177, 2020.

[4] R. J. Hassan, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, et al., "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions," Asian Journal of Research in Computer Science, pp. 32-48, 2021.

[5] Z. Ageed, M. R. Mahmood, M. Sadeeq, M. B. Abdulrazzaq, and H. Dino, "Cloud computing resources impacts on heavy-load parallel processing approaches," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 22, pp. 30-41, 2020.

[6] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," Optics & Laser Technology, vol. 124, p. 105942, 2020.

[7] M. A. Sadeeq, S. R. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things security: a survey," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 162-166.

[8] M. M. Sadeeq, N. M. Abdulkareem, S. R. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and Cloud computing issues, challenges and opportunities: A review," Qubahan Academic Journal, vol. 1, pp. 1-7, 2021.

[9] H. Yi, "Systolic inversion algorithms for building cryptographic systems based on security measurement in IoT-based advanced manufacturing," Measurement, vol. 161, p. 107827, 2020.

[10] I. B. Djordjevic, "On global quantum communication networking," Entropy, vol. 22, p. 831, 2020.

[11] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq, S. F. Kak, Z. N. Rashid, A. A. Salih, et al., "A survey of data mining implementation in smart city applications," Qubahan Academic Journal, vol. 1, pp. 91-99, 2021.

[12] V. Hassija, V. Chamola, A. Goyal, S. S. Kanhere, and N. Guizani, "Forthcoming applications of quantum computing: peeking into the future," IET Quantum Communication, vol. 1, pp. 35-41, 2020.

[13] Z. Hu, R. Xia, and S. Kais, "A quantum algorithm for evolving open quantum dynamics on quantum computing devices," Scientific reports, vol. 10, pp. 1-9, 2020.

[14] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," IEEE Transactions on Multi-Scale Computing Systems, vol. 1, pp. 99-109, 2015.

[15] S. K. Routray, et al., "Quantum cryptography for iot: Aperspective," in 2017 International Conference on IoT and Application (ICIOT), 2017, pp. 1-4.

[16] C. Badertscher, A. Cojocaru, L. Colisson, E. Kashefi, D. Leichtle, A. Mantri, et al., "Security limitations of classical-client delegated quantum computing," in International Conference on the Theory and Application of Cryptology and Information Security, 2020, pp. 667-696.

[17] B. C. Britt, "Modeling viral diffusion using quantum computational network simulation," Quantum Engineering, vol. 2, p. e29, 2020.

[18] M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," IEEE Communications Magazine, vol. 51, pp. 36-41, 2013.

[19] C.-Y. Chen, G.-J. Zeng, F.-J. Lin, Y.-H. Chou, and H.-C. Chao, "Quantum cryptography and its applications over the internet," IEEE Network, vol. 29, pp. 64-69, 2015.

[20] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," Future Generation Computer Systems, vol. 86, pp. 951-960, 2018.

[21] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," IEEE Access, vol. 6, pp. 1073-1081, 2017.

[22] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, et al., "Present landscape of quantum computing," IET Quantum Communication, vol. 1, pp. 42-48, 2020.

[23] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, et al., "Quantum computing: A taxonomy, systematic review and future directions," arXiv preprint arXiv:2010.15559, 2020.

[24] Z. S. Ageed, R. K. Ibrahim, and M. Sadeeq, "Unified ontology implementation of cloud computing for distributed systems," Current Journal of Applied Science and Technology, pp. 82-97, 2020.

[25] B. M. Boghosian and W. Taylor IV, "Simulating quantum mechanics on a quantum computer," Physica D: Nonlinear Phenomena, vol. 120, pp. 30-42, 1998.

[26] K. Bertels, A. Sarkar, T. Hubregtsen, M. Serrao, A. A. Mouedenne, A. Yadav, et al., "Quantum computer architecture: Towards full-stack quantum accelerators," in 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2020, pp. 1-6.

[27] R. Feynman, "Simulating Physics with Computers, 1982, reprinted in: Feynman and Computation," ed: Perseus Books, 1999.

[28] Y. S. Jghef and S. Zeebaree, "State of art survey for significant relations between cloud computing and distributed computing," International Journal of Science and Business, vol. 4, pp. 53-61, 2020.

[29] U. Alvarez-Rodriguez, M. Sanz, L. Lamata, and E. Solano, "Quantum artificial life in an IBM quantum computer," Scientific reports, vol. 8, pp. 1-9, 2018.

[30] H. M. Yasin, S. R. Zeebaree, M. A. Sadeeq, S. Y. Ameen, I. M. Ibrahim, R. R. Zebari, et al., "IoT and ICT based smart water management, monitoring and controlling system: A review," Asian Journal of Research in Computer Science, pp. 42-56, 2021.