Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020780
Article

Tech Science Press

Analyzing the Data of Software Security Life-Span: Quantum Computing Era

Hashem Alyami[1], Mohd Nadeem[2], Wael Alosaimi[3], Abdullah Alharbi[3], Rajeev Kumar[4,*], Bineet Kumar Gupta[4], Alka Agrawal[2] and Raees Ahmad Khan[2]

[1]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Computer Applications, Shri Ramswaroop Memorial University, Barabanki, 225003, India
*Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com

Received: 21 May 2021; Accepted: 22 June 2021

Abstract: Software or web application security is the main objective in the era of Information Technology (IT) and Artificial Intelligence (AI). Distinguishing proof of security at the initial stage produces significant results to comprehend the administration of security relics for best potential outcomes. A security alternative gives several methods and algorithms to ensure the software security. Security estimation is the vital factor in assessing, administrating, controlling security to improve the nature of security. It is to be realized that assessment of security at early stage of development helps in identifying distinctive worms, dangers, weaknesses and threats. This paper will talk about the definition and characterization of quantum computing in software security. For software security, we use different cryptography (methods or algorithms to secure our financial organizations, medical devices, military weapons, planes, ships, automobiles, navigators, etc. However, many cryptosystems are likely to collapse when the large quantum computer is developed. Recently, Google developed the *Sycamore Processor 53 qubit*s. Such innovations indicate the advent of large quantum computer in future. Since cryptographic algorithm can be solved by the quantum computers, the present cryptosystem would be rendered obsolete. Hence, it is imperative to focus more on intensive research in the context of the present quantum cyber security. The main challenges in quantum era would be cryptography methods that fulfill the demands of security usability and flexibility without sacrificing the users' confidence. This research study, in particular, focuses on 'Software durability' which is a quality of security that alludes to the capacity to execution of an item on schedule. In the context of software and web application, a thorough assessment of security factors will significantly influence the software's durability in the era of quantum computing.

Keywords: Software security; quantum technology; cryptography methods; cryptosystems; quantum computing

1 Introduction

Quantum computing is a groundbreaking technology in the field of IT that can support the global efforts in addressing the security of software and the web application. Software with compromised strength is probably going to fizzle in a profoundly serious market; hence, software creating associations are focusing harder towards guaranteeing the sturdiness of their products. Software improvement life cycle contains numerous stages, for example, necessities designing, plan, coding and testing. Upkeep is viewed as the last phase of advancement [1].

Functionality of software can be characterized as the conditions in which programming is as yet helpful or viable. Usefulness of software ought to be strong so as to accomplish viability. Sturdiness in the software is the time-frame for which programming is giving administrations [2]. The advancing adaptable climate in the mid twenty-first century makes new difficulties for all, including the product [3,4]. Quantum security deals with the security in the era of quantum computing. Nowadays the rate of development of quantum technology is exponential. A group of scientists have successfully developed a fully quantum processor, *Sycamore Processor* which designs the quantum circuit in 200 s, something that could have been done by the classical supercomputer in 10,000 years [5].

With the development of quantum processor, the current structure of encryption or security methods of different networks, web applications, software, financial structure of encryption, security in defense and everything that is based on computer network is at stake, the durability of software is also affected by quantum computer. The present security mechanisms in the classical computers are symmetric and asymmetric. In a symmetric approach, the same key is used to encrypt data and decrypt data. While in the asymmetric approach, different keys are used. The security is totally based on security key which is in the form of integer number as per the *Shor* algorithm. The large number of size 2042 bit can be factorized to its prime number [6]. The total time taken by the classical computer can be factorized of break by 100 year. However by the use of quantum phenomenon, principally, it can be broken down within few minutes.

The rest of the paper is structured as follows: In Section 2, the literature perused for profiling this research has been explained. In Section 3, operation of quantum has been explained in the form of qubit. Section 4 explains the software security issues in the quantum computing era. Section 5 dwells on the challenges of software security in quantum computer era and mentions the existing quantum security algorithm. Section 6 presents the conclusion of our review in quantum computing era.

2 Related Works

Several research studies have been done on quantum computing and software security explicitly, the combined approaches are supposed to be novel and these have been mentioned in our review paper. In the last decade, the researchers focused on the development of quantum computer, the different algorithms of quantum computing to enhance the computing phenomenon. The complex algorithms of cryptography have been resolved by the quantum computing in seconds. The present security technique of classical computer and super computer security methods have collapsed in quantum computing era. Our research has specifically underlined the issues and challenges of software security in the quantum era. While profiling our research, the relevant literature sources that we referred to in particular on the software security and quantum computing have been detailed below:

Mitra et al. [7] state that Quantum Cryptography is the most promising cryptographic field for quicker, powerful and safer correspondences. Quantum security mechanism covers quantum properties of light under quantum mechanics on cryptographic undertaking rather than present status of calculations dependent on numerical figuring innovation. Major calculations for public key encryption and a few computerized signature plans, for example, RSA, El Gamal cryptosystem, hash work is defenseless at quantum foes.

A large portion of the considering issue can be broken by Shore's calculation and quantum PC compromises other hand discrete logarithm issue.

Abomhara et al. [8] mention that the Internet of Things (IoT) gadgets are quickly getting omnipresent while IoT administrations are getting unavoidable. Their prosperity has not gone unnoticed and the quantity of dangers and assaults against IoT gadgets and administrations are on the increment also. Digital assaults are not new to IoT, however as IoT will be profoundly entwined in our lives and social orders, it is getting important to pay attention to digital safeguards. Henceforth, there is a genuine need to get IoT, which has subsequently brought about a need to extensively comprehend the dangers and assaults on IoT framework.

Ma et al. [9] cite that the Quantum key conveyance permits distant gatherings to create data hypothetical secure keys. The bottleneck choking its genuine applications lies in the restricted correspondence distance and key age speed because of the way in which the data transporter is lost in the channel. For all the current usage, the key rate is limited by the channel's transmission probability. Or maybe shockingly, by coordinating the periods of two sound states and encoding the vital data into the normal stage, this direct key-rate limitation can be survived—the protected key rate scales with the square base of the transmission probability, as proposed in twin-field quantum key circulation. To accomplish this, the researchers build up optical-mode-based security evidence that is not the same as the ordinary qubit-based security confirmations. Besides, the proposed plot is estimation gadget free, i.e., it is resistant to all conceivable recognition assaults. The reproduction result shows that the key rate can even surpass the transmission probability between two correspondence parties. Moreover, researcher apply stage post compensation to devise a more conversant form of the plan without stage locking, which makes the proposed conspire doable with the current innovation. This implies that quantum key conveyance can appreciate both the sides of, commonsense and security at the same time.

Zheng et al. [10] observe that the quantum correspondence has broadly evolved in the course of recent years. As a significant part of quantum correspondence, quantum secure direct correspondence advances high security and promptness in correspondence by directly communicating messages over a quantum channel. The full usage of a quantum convention consistently requires the capacity to control the exchange of a message successfully in the time area; consequently, it is fundamental to join quantum secure direct correspondence with quantum memory to achieve the correspondence task. In this Letter, they report the trial exhibit of quantum secure direct correspondence with cutting edge nuclear quantum memory without precedent for guideline. They utilize the polarization levels of opportunity of photons as the data transporter, and the constancy of trap unraveling is checked. The work finishes a basic advance toward common sense quantum secure direct correspondence and exhibits a likely application for significant distance quantum correspondence in a quantum organization.

The methodologies examined above give information about the security of software in quantum computing era. In the ensuing segment, we have talked about various software security contexts and quantum computing era. The concepts will be an effective base for organizing the software security more efficiently.

3 Quantum Security

The present trend of the development of quantum technology predicts a progressive trajectory in future that is more likely to witness the exponential growth of quantum processor *2 qubits to 53 qubits* [11]. Quantum security can be classified into three categories which are shown in Fig. 1.

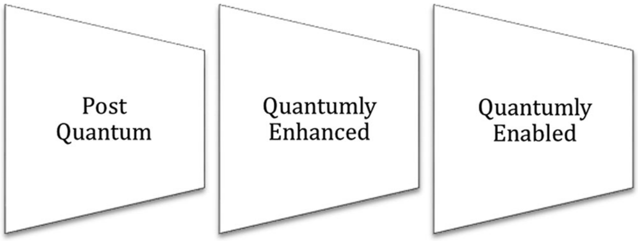

Figure 1: Schematic representation of quantum security

3.1 Post Quantum Cryptography

The post quantum approach of security means that the user has few algorithms by which we can ensure the security in quantum computing era. The post quantum cryptography's purpose is to achieve usability, flexibility without losing the confidence of the user. In future, when the quantum computer will be in existence, the present security procedure such as RSA, DSA and ECDSA will be ineffectual. For the working principle of cryptography, the developers have generated two keys: the public key and the private key [12]. The private key cannot disclose the algorithm of the public key transfer, thus securing the channel for the user. User uses it as per requirement and the system is secure at present. But with the development of the Quantum technology, it will be fairly easy to break the present cryptographic algorithm. The development of quantum technology by *P. Shor* of *Shor a*lgorithm has proven to be a path breaking discovery. The principle of cryptography is based on the keys which are a collection of integers that cannot be known without the keys. As per the cryptography principle, we have a public key and a private key which are a collection of integers or hexadecimal codes. By the use of random selection we make keys of different sizes. The size is the function of hardness and by increasing the size; we make the cryptography algorithm strong, which is difficult to break. Breaking the cryptography is the function of time, so the key size breakability is directly proportional to the time. If we consider key size as $k(n)$ and time$t$, $k(n) \propto t$, then, both the key and time function is directly proportional to each other. If we increase the key size, the time will also increase and the cryptographic algorithm will be considered secure. But by the recent development of the *Sycamore Processor* (quantum technology), these calculations will be solved within minutes. Solutions that could only be accomplished by the classical computer in 10000 years would be done in miniscule time in the era of quantum technology [13]. With large qubits quantum computers in existence, the security of the entire data exchanged through online communication would be at risk. The quantum Cyber Security would be at a higher risk, were we to develop 200 or more qubits quantum computer. Right now Google and IBM have developed the 53 qubits quantum computer. Though not an imminent debacle at present, the security of data and financial sector ensured by the current cryptography technique needs major improvisations.

3.2 Quantum Enhanced Cryptography

Quantum computer makes the cryptography method obsolete. The quantum enhanced approach is the procedure of assumption in which the quanta technologies are developed to a small level and cannot break the encryption algorithm like AES, DES etc. The present cryptographic algorithms are working efficiently but the development of security in quantum era would need stronger processes. In the context of quantum enhanced scenario, the cryptography process data will be secured by the key. The quantum key distribution is the new methodology of the network encryption in which the developer uses the uncertainty principle of matter to ensure that the data cannot be interfered with by the hacker [14]. The quantum cryptography approach, which deals with different quantum distribution keys, mathematical based approach such as lattice based cryptographic approach, hash based signature and code based are useful for security of software and web application. The following approaches ensure the software durability. Quantum cryptography will ensure the security of software and also ensure the durability of the software.

3.3 Quantum Enabled Cryptography

The approaches of quantum enabled cryptography means that the large quantum computers being developed have the computation power for breaking the current security encryption procedure. The exponential development of quantum computer needs the current cryptographic procedure upgradation. The mentioned quantum algorithm will ensure the durability and security of software. The basic difference between the classical computer and quantum computer are its operation on bit and qubits. Bits operates with 1 and 0 operation at two different time lines, while in quantum computer the qubits operate 1 and 0 at the same time by the use of superposition principle and entanglement [15]. Fig. 2 illustrates the entanglement of photon; here two photons are rotating in spin circularly, which *indicate both* logics at the same time 0 and 1 as per Boolean algebra.

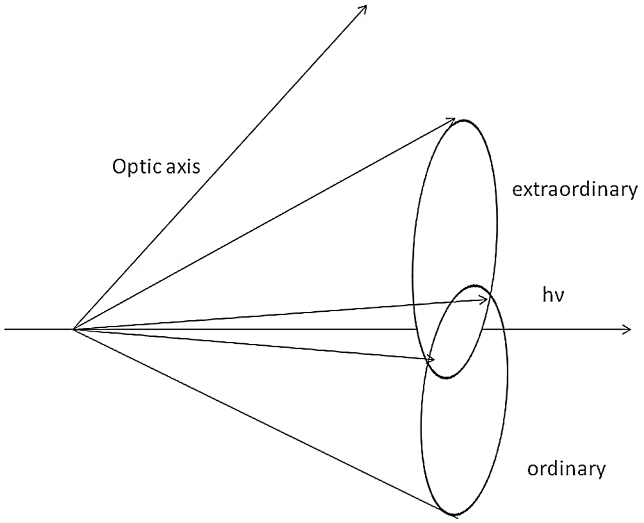

Figure 2: Entanglement of photon

Working Operation of quantum computer is based on qubit algebra. In quantum computing, the qubits shows both the states of operation 1 and 0 at the same time by the use of superposition principle and entanglement. An atmosphere of spectacular secret appends to the idea of quantum entanglement, and furthermore to the (by one way or another) related case that quantum hypothesis requires "numerous universes." Yet in the end those are, or ought to be, logical thoughts, with rational implications and solid ramifications.

Trap is frequently viewed as an interestingly quantum-mechanical marvel, however it isn't. Truth be told, it is edifying, however fairly unusual, to think about a basic non-quantum (or "old style") form of trap first. This empowers us to decipher the nuance of entanglement itself as separated from the overall peculiarity of quantum hypothesis. This means that the working photon (basic entity of matter/computing) can show both the states at the same time, as shown below.

Fig. 2, shows the surface of sphere in which the photon exists. It is seen that it is continuously spinning and shows both the values at the same time. Let us explain its operation with an example—if we choose to move from one location to another, we may have four different routes for the same. The present classical approach differentiates the route as per the condition of short distance, long distance or any other condition. Thereafter whichever condition fulfills the criteria, that specific route is selected. This example explains the classical computing approach. In the quantum computing approach, all the possible routes have been fulfilled by qubits at the same time and one can reach the destination by any of these routes. This example shows us that since the quantum computing technology chooses all the fields at the same time, so the process is less time consuming.

4 Operations of Qubits

The quantum computing is differing from the classical computer because of its basic operation which is based on Q algebra (Quantum algebra). The qubits (φ) are defined in the mathematical expression as:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

The bracket notation $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and α, β are the complex number then

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

That shows the $|\alpha|^2 = 0$ then $|\beta|^2 = 1$ or $|\alpha|^2 = 1$ then $|\beta|^2 = 0$. Let us consider U as unitary matrix and U' its transpose-

$$UU' = U'U = I \tag{3}$$

I, is the identity matrix.

$$|\varphi\rangle = U|\varphi\rangle = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} U_{00}\alpha + U_{01}\beta \\ U_{10}\alpha + U_{11}\beta \end{pmatrix} \tag{4}$$

The state of qubits is defined as a tensor product $\otimes$ (it is multiplication of two vector spaces). This is defined as: $|\gamma_j\rangle = \alpha_j|0\rangle + \beta_j|1\rangle$, for $j = 1, 2, 3$.

The tensor product of joint state is

$$|\gamma_1\gamma_2\gamma_3\rangle = \gamma_1 \otimes \gamma_2 \otimes \gamma_3$$

$$= \alpha_1\alpha_2\alpha_3|000\rangle + \alpha_1\alpha_2\beta_3|001\rangle + \alpha_1\beta_2\alpha_3|010\rangle + \alpha_1\beta_2\beta_3|011\rangle + \beta_1\alpha_2\alpha_3|100\rangle + \beta_1\alpha_2\beta_3|101\rangle + \beta_1\beta_2\alpha_3|110\rangle + \beta_1\beta_2\beta_3|111\rangle \tag{5}$$

Eq. (5) shows that the three inputs will result in eight output as well as n input to 2^n output. Qubits can mathematically be represented by unitary function, so the number of input is equal to the number of output qubits.

5 Software Security Issues

Software security is a major concern in the field of quantum computing. The rapid progress in Quantum technology will require inventive and highly efficacious approaches in cyber security domain. The encryption and decryption methods can easily be matched by the qubits combination at the same time. Few more pertinent issues are underlined below:

- Google's Sycamore Quantum Processor can calculate the 10000 year large calculation in just 200 s so the encryption key of data can be invaded easily.
- The encryption of Wi-Fi can be cracked in seconds.
- The development of qubits is exponential. Already 53 qubits have been developed, if we reach 2000, the security of todays encryption will be broken.

- The different methods of security in quantum computing are very costly.

The different cryptographic approach and the post quantum algorithm which can break the present encryption algorithm are mentioned in Tab. 1.

Tab. 1 shows the different cryptographic algorithms which will be broken by the *Grover* algorithm and the *Shor* algorithm in the quantum era. They must be revised or replaced by improvised ones so as to contend with the future challenges of cybersecurity.

Table 1: Cryptographic method/function and its post quantum algorithm

Name of encryption	Function	Present security	Quantum security
	Symmetric		
Advanced encryption standard-128	SE	128	64 (Grover)
Advanced encryption standard-256	SE	256	128 (Grover)
Salsa-20	SE	256	128 (Grover)
SHA-256	HashFunction	256	128 (Grover)
SHA-3256	HashFunction	256	128 (Grover)
	Key Cryptography		
RSA 3072	Encryption	128	Broken (Shor)
RSA 3072	Signature	128	Broken (Shor)
DH 3072	Key exchange	128	Broken (Shor)
DSA 3072	Signature	128	Broken (Shor)
ECDH 256	Key Exchange	128	Broken (Shor)
ECDSA 256	Signature	128	Broken (Shor)

6 Challenges in Software Security in the Quantum Computing Era

As analyzed above, it is evident that the quantum computing development progress makes the present cryptography algorithm insecure by its operational speed. This poses to be a major challenge. Few of the cryptographic procedures which can be enlisted to address these challenges are:

6.1 Lattice Based Cryptographic Algorithm

In context of the post quantum cryptography, this method promises to secure the data or information against the quantum computing [16]. Hoff stein, Pipher and Silverman introduced the Lattice based encryption which is unbroken today. The lattice structure is an n dimensional periodic space in which the n dimensional vector b1, ……bn $\in \mathcal{R}^n$, the lattice generated is a set of vectors,

$$\mathcal{L}(\mathrm{b1}, \ldots \mathrm{bn}) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\} \tag{6}$$

The vector b1, b2…bn are known as basic lattices [17]. Here $\mathbb{Z}$ is the random class of lattice, $\mathcal{R}$ is the set of real number and $\mathcal{L}$ is the length of lattice [18]. The multidimensional lattice structure is shown in Fig. 2. The problems of lattice based cryptography are: Short Vector Problem and LLL Algorithm. In SVP, input lattice is arbitrary and its approximation is short. In 1982, researcher lenstra gave the LLL algorithm. This algorithm has the approximation in $2^{O(n)}$, where n is the size of lattice.

6.2 Fully Homomorphic Algorithm

In the homomorphic encryption, without revealing the data, the data between two parties can be manipulated by anyone but cannot be revealed [19]. We can understand this concept by the example of an election procedure. An election has two main stakeholders or parties- the people and the leaders for whom the people vote. The election commission is the third party in this context which can count the number of votes casted for each leader, but cannot reveal it before the assigned time. Thus, the data is in public domain but cannot be revealed by the third party as in the case of Homomorphic encryption. The major advantage of Homomorphic encryption is that it cannot be broken in the post quantum era. Homomorphic encryption algorithm follows the public key to encrypt the data, while for the decryption we use the algebraic function to solve the encryption algorithm and decrypt the algorithm. The decryption process by algebraic function cannot be broken by the quantum computer.

6.3 Quantum Key Distribution

Quantum key distribution is the transmission of data known as encryption key with the help of qubits which have unique behavior as against the classical computer system [20]. Till the previous year, the quantum key distribution needed a separate fiber optic line for the information transfer, but at present, they can be transferred from the existing fiber optic line. This reduces the cost of communication. There is another communication based on satellite communication. This mode of communication is based on Einstein hypothesis and is called the '*spooky action at a distance'* [21]. For the past few years, China has been working on quantum communication satellite. The communication principle is the entanglement; it is the process in which the photons spin individually. When we correlate the spinning of the photons, then both have a relation. If this relation is not the sending message to each other, it means that they can generate a random number which can be used in encryption algorithm. This methodology of encryption is very costly.

7 Future Scope of Quantum Software Security

Since the cryptographic algorithm used in cybersecurity will be ineffective with the advent of quantum computer, the researchers need to work on converse solutions to this problem. Lattice based cryptographic algorithms can be considered to be the most apt process in this regard [22]. Lattice based algorithm involves hiding of the cryptographic data into a complex algebraic mathematics functions. It is the basis of another encryption methodology, named Fully Homomorphic Encryption (FHE) [23]. FHE can be best understood by the example of a medical report of a patient. Once this report is encrypted by FHE, it will be transmitted from one doctor to another without revealing the name of the patient. In short, we can hide the encryption key of the cryptographic algorithm [24]. The lattice based cryptographic algorithm does not have a standard library of encryption algorithm and is, yet, years away from commercial software.

8 Conclusion

Quantum computing applications are as of now developing across the globe. Different difficulties and worries around quantum computing require an exhaustive report on this subject. This paper reviewed the fundamental components of quantum computing and further investigated the capability of quantum processing to improve scientific and figuring capacities in tackling software security and durability. It is obvious that producing a completely secure framework is beyond the realm of imagination; subsequently, it can't be considered as the goal of assessing software sturdiness to be the boundaries of great and secure software. Hence, the goal is to diminish the support issue for long time workable software. Focus on strengthening the software durability from the very beginning of the development cycle will raise the degree of value in the product. In this article, we mentioned the quantum approach and software durability. The quantum safe algorithm will secure the quantum attack on present encryption security approach. However, whether it is the Lattice based quantum algorithm or any other, there can be no guarantee for foolproof security in the context of online communication. Yet, in the wake of the development of quantum computer, Lattice based quantum algorithm is decidedly an effective improvisation.

Acknowledgement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/254), Taif University, Taif, Saudi Arabia.

Funding Statement: This Project was funded by the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia, under Grant Number: TURSP-2020/254.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Kelty and S. Erickson, “The durability of software,” *Meson Press*, vol. 1, no. 5, pp. 1–13, 2015.

[2] E. Nathan, “When good software goes bad: The surprising durability of an ephemeral technology,” in *Proc. Mistakes, Ignorance, Contingency, and Error Conf.*, Munich, Germany, pp. 1–16, 2014, [Online]. Available: https://larlet.fr/static/david/blog/ensmenger-maintainers-v2.pdf.

[3] D. G. Firesmith, “Common concepts underlying safety-security and survivability engineering,” *Software Engineering Institute*, vol. 1, no. 1, pp. 1–75, 2003.

[4] S. Becker, M. Boskovic and A. Dhama, “Trustworthy software systems: A discussion of basic concepts and terminology,” in *Graduate School Trustsoft Carl-von-Ossietzky University of Oldenburg*. Germany, pp. 1–30, 2006.

[5] F. Arute, K. Arya and R. Babbush, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 1, pp. 505–510, 2019.

[6] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[7] S. Mitra, B. Jana, S. Bhattacharya, P. Pal and J. Poray, “Quantum cryptography: Overview, security issues and future challenges,” in *Proc. 4th Int. Conf. on Opto-Electronics and Applied Optics (Optronix)*, Kolkata, India, pp. 1–7, 2017.

[8] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks,” *Journal of Cyber Security and Mobility*, vol. 1, no. 1, pp. 65–88, 2015.

[9] X. Ma, P. Zeng and H. Zhou, “Phase-matching quantum key distribution,” *Physical Review*, vol. 8, no. 3, pp. 31–43, 2018.

[10] W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, S. B. Shi *et al.,* “Quantum secure direct communication with quantum memory,” *Physical Review Letters*, vol. 118, no. 22, pp. 220–501, 2017.

[11] X. Pang, L. Feng, L. Zhou, K. Liu, A. L. Yang *et al.,* “Experimental quantum-enhanced cryptographic remote control,” *Scientific Reports*, vol. 9, no. 1, pp. 1–10, 2019.

[12] M. Ajtai, “Generating hard instances of lattice problems in complexity of computations and proofs,” *Quad Mathematics*, vol. 16, no. 1, pp. 1–32, 2004.

[13] J. Sen, “Homomorphic encryption-theory and practice of cryptography and network security protocols and technologies,” *IntechOpen*, vol. 1, no. 1, pp. 1–10, 2013.

[14] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-Quantum Cryptography*, vol. 1. Berlin, Heidelberg, pp. 1–10, 2009.

[15] M. Alenezi, M. Nadeem, A. Agrawal, R. Kumar and R. A. Khan, “Fuzzy multi criteria decision analysis method for assessing security design tactics for web applications,” *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 5, pp. 181–196, 2020.

[16] T. Ladd, F. Jelezko and R. Laflamme, “Quantum computers,” *Nature*, vol. 464, no. 5, pp. 45–53, 2010.

[17] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* “A knowledge based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security durability of web applications,” *IEEE Access*, vol. 8, no. 8, pp. 48870–48885, 2020.

[18] D. Micciancio and O. Regev, “Lattice-based cryptography,” *Nature*, vol. 2, no. 2, pp. 1–20, 2017.

[19] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni and M. O’Neill, “On practical discrete Gaussian samplers for lattice-based cryptography,” *IEEE Transactions on Computers*, vol. 67, no. 3, pp. 322–334, 2018.

[20] N. S. Prabhjot and H. Kaur, “A review of information security using cryptography technique,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 1, pp. 323–326, 2017.

[21] B. Preneel, “Understanding cryptography: A textbook for students and practitioners,” *IEEE Transactions on Computers*, vol. 1, no. 5, pp. 1–10, 2010.

[22] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, “A review paper on network security and cryptography,” *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 763–770, 2017.

[23] A. Gupta and N. K. Walia, “Cryptography algorithms: A review,” *International Journal of Engineering Development and Research*, vol. 2, no. 2, pp. 1667–1672, 2014.

[24] J. Callas, “The future of cryptography,” *Information Systems Security*, vol. 16, no. 1, pp. 15–22, 2007.