ISSN: 2583-7354

I J E K S
Open Knowledge

International Journal of
Emerging Knowledge Studies
Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

A SURVEY ON 'QUANTUM COMPUTING' APPLICATIONS TO BOLSTER SECURITY IN THE "INTERNET OF THINGS (IOT)'

Dr. Kirti Diddi[1], Er. Sachin Upadhyay[2], Er. Kevin Dcruz[3]*
[1]Principal of Nirmala College & Academic Director of Nirmala College of Education, Ujjain (M.P.), India.
[2]Assistant Professor, Nirmala College, Ujjain, India.
[2]System Administrator, Nirmala College, Ujjain, Madhya Pradesh, India.
*Corresponding Author: ittech.net@gmail.com

Article Info: - Received : 09 December 2023 Accepted : 18 December 2023 Published : 30 December 2023

Abstract

The term 'Internet of Things (IoT)' refers to a massive collection of connected things that may exchange data and information over a computer network, such as the Internet. These things consist of a blend of sensors, physical components, and a device to control the process of functioning of various chunks of the unit. Individually object uses sensors to collect and transmit information from its immediate environment to additional objects or a centralize database over a network. The security of these linked IoT plays a pivotal role with limited margin for error is a major challenge in the field of IoT. It is a significant concern for all organizations that employ IoT technology. 'Quantum Computing', built on the principles of quantum mechanics, has the capability to provide a substantial benefit over conventional computing. The positive aspect of 'Quantum Computing' is that it offers solutions to numerous previously unsolvable challenges in the fields of secure communication and finance. The present IoT security uses 'cryptographic algorithms' like 'Rivest-Shamir-Adleman (RSA)' & 'elliptic curve cryptography (ECC)'. The safety of such computations is profoundly affected by 'Quantum Computing'. We investigate the vulnerabilities of quantum-based solutions and IoT smart applications. This study evaluates and discusses the most vital issues regarding security in the field of the 'IoT', while also considering the significant impact of quantum computers.

Keywords: *Cryptographic Algorithms, 'Quantum Computing', IoT.*

1. INTRODUCTION

The rapid proliferation of diverse internet-connected electronic devices serves as compelling evidence for IoT technology. HCAC (Heating, Ventilation, and Air Conditioning) systems and Thermostats found in smart houses are examples of this technology, as they regulate and oversee the heating and cooling systems. The 'Internet of Things (IoT)' contributes substantially to the improvement of mankind through addressing and simplifying various aspects of human existence, ultimately leading to an improved quality of life. These applications encompass smart car technology and address the potential damage caused by natural disastersor human activities [1]. The utilization of 'Internet of Things (IoT)' is proliferating in applications including cities, smart grids, and intelligent system. 'Internet of Things (IoT)' communication's proliferation of linked gadgets enables consumers with enhanced decision-making capabilities. The wide range of applications offered by IoT, as depicted in Figure 1, involve the transport of a significant volume of data, leading to security and privacy concerns. Authentication and privacy are essential for ensuring the proliferation of IoT applications. Additionally, it has the potential to pose weighty security dangers to its probable users. The 'Internet of Things (IoT)' presents issues in domains such as confidentiality, secrecy, and authentication. The current state of 'IoT' related applications relies on ECC and RSA based practice(s)[2].

Fig-1: Futuristic IoT Architecture

The IoT integrates several technologies, such as smartphones, household appliances, radio frequency identification (RFID), sensors, and others. Furthermore, every IoT device possesses a distinct identification that enables seamless communication between devices via the Internet. This autonomous capability empowers them to make independent decisions without human intervention [3]. Hence, the 'Quantum Computing' technology ensures safety of this 'IoT Communication Network'.

'Quantum Computing' relies on the fundamental concepts of uncertainty [4] and 'No-cloning Theorem' [5]. 'The Internet of Things (IoT)' not only revolutionizes data interchange but exerts significant influence on the physical realm. In the foreseeable future, marketing gadgets that lack internet connectivity will become obsolete. Furthermore, it is projected that 'Internet of Things (IoT)' devices will exert significant influence over multiple trillions of global economies by the year 2020. Nevertheless, the security concerns around the 'Internet of Things(IoT)' have yet to be resolved.

Bruce Schneider, a distinguished security specialist affiliated with Harvard University and serving as the CTO of IBM Resilient, maintains that manufacturers of 'IoT' devices continue to prioritize cost-effectiveness above enhancing their security protocols. The Ukraine power grid attacks, which utilized IoT technologies to manipulate lighting controls, unequivocally demonstrate the potential for evil individuals to plunge human existence into darkness. The researchers focused solely on highlighting the flaws of IoT security, neglecting to consider the significant impact of 'Quantum Computing', which should have been taken into account [6]. Classical computing operates by manipulating individual bits, but 'Quantum Computing' utilizesqubits.

The quantum state is represented by these qubits, together with their corresponding probabilities. These 'Qubits' are built on fundamental concepts of 'Quantum Mechanics', such as 'Entanglement' and 'Superposition'. Superposition permits 'Qubits' to exist in an infinite number of simultaneous value combinations. A strong and mutually reliant bond between quantum particles is created by Entanglement. However, the advancement of 'Quantum Computing' poses a serious threat to existing encoding protocols.

'Quantum Key Distribution (QKD)' is a prominent field of study within the realm of 'Quantum Computing'. It allows the parties involved in communication to establish confidential keys for secure communication. 'Quantum Computing' offers numerous advantages to the future society, including the development of life-saving pharmaceuticals, the advancement of artificial intelligence, and the creation of intelligent infrastructure. 'Quantum Computing' progressions offer risks to cyber security algorithms. As the 'Internet of Things (IoT)' continues to expand at a rapid pace, there has been a lot of research on how to keep these embedded systems safe, particularly wireless sensor networks (WSNs). Employing asymmetric cryptography is crucial for ensuring the security of data exchange.

However, its implementation in IoT systems is challenging due to the excessive resource requirements. Employing complicated 'Encryption Algorithms' in 'IoT' systems leads in device overheating, poor processing, longer execution time, and increased power usage. So, these algorithms are not appropriate for such systems. An advanced configuration for Wireless Sensor Networks (WSNs) consists of an 8 or 16-bit micro-controller operating at a rate of up to 10 Mega Hertz. It has a limited memory of RAM, typically a few kilobytes, and a secondary memory of 256 kilobytes to store the executable software. In addition, the restrictions on processing power and energy constraints in IoT devices pose significant challenges that must be taken into account when implementing cryptography algorithms. Typically, wireless sensor networks (WSNs) operate using two AA-sized batteries for extended periods of time, ranging from months to years, without requiring recharging or replacement [8].

'Quantum Computing' has emerged as one of the top 10 cutting-edge technologies in recent years. Renowned corporations like Microsoft, Intel, Google and IBM are investing in the development of the original general-purpose Quantum Computer. A sophisticated CPU and 72 qubits make this computer noteworthy that has a specification of 2048 qubits [9]. Concurrently, significant work has been done to developing a programming set of instructions specifically for 'Quantum Computers'. Several projects have already been established, like Q# by Microsoft and OpenQASM by IBM. Additionally, there are SDKs available, such as QISKit by IBM, as well as 'Quantum Computing' simulators like Open Fermion and QuTip.

In addition, cloud-based 'Quantum Computing' services such as IBM Q Experience make it possible for programmers to run their programs on quantum computers via the Internet, facilitating scientific experiments and educational endeavors. Yet, quantum computers still face numerous unresolved challenges; yet, they represent a groundbreaking era in terms of computational capabilities. Furthermore, it exposed numerous vulnerabilities in the field of cybersecurity, particularly in IoT systems, due to their inherent resource limitations [9]. This paper's main goals and reasons for being are to explain what the IoT is and how essential it is in this day and age, look at IoT security in detail, and talk about the newest important research on IoT security.

A survey is done to analyze the security of IoT smart applications, focusing on the problems associated with IoT security and 'Quantum Computing'. The primary obstacles to implementing a 'Quantum Computing'-based Internet of Things (IoT) cryptosystem are outlined.

2. LITERATURE SURVEY

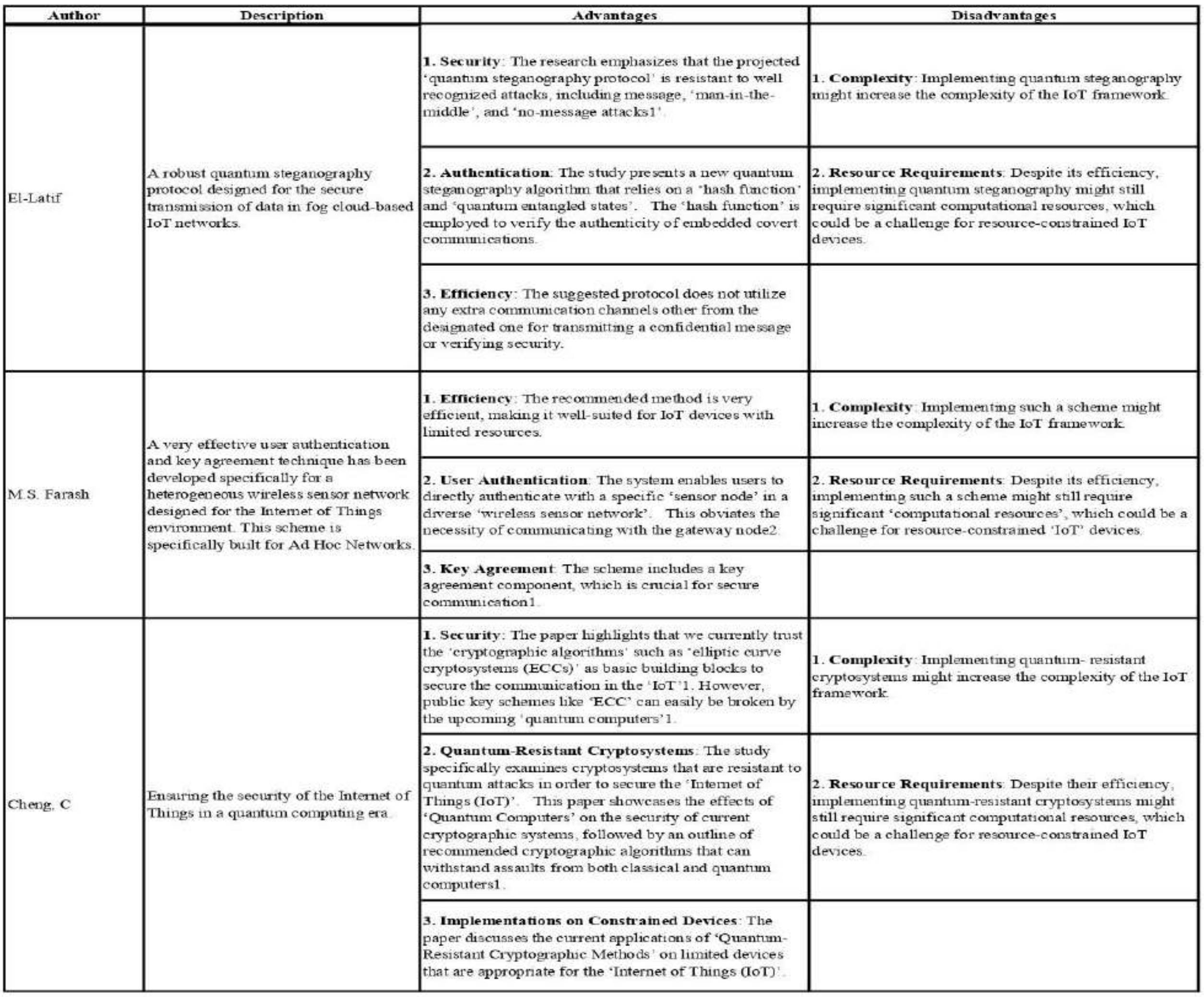
Recently, numerous researchers have focused on addressing security issues and proposing solutions for IoT devices. This section of the study will discuss the key findings from recent research studies. Every device establishes communication over the internet. Farash et al. [10] introduced a validation procedure in which operators are granted access to data only if they successfully complete the authentication and key agreement methods. Mitchell et al. [10] employ cryptography to examine the ramifications of 'Quantum Computers' on established 'Cryptographic Primitives'. Cheng et al. [11] focused their investigation on the latest advancements in quantum cryptography for safeguarding IoT devices. The significant advancements in 'Quantum Computing' in recent years have necessitated the development of a strategy to safeguard inter-communication among 'IoT' devices.

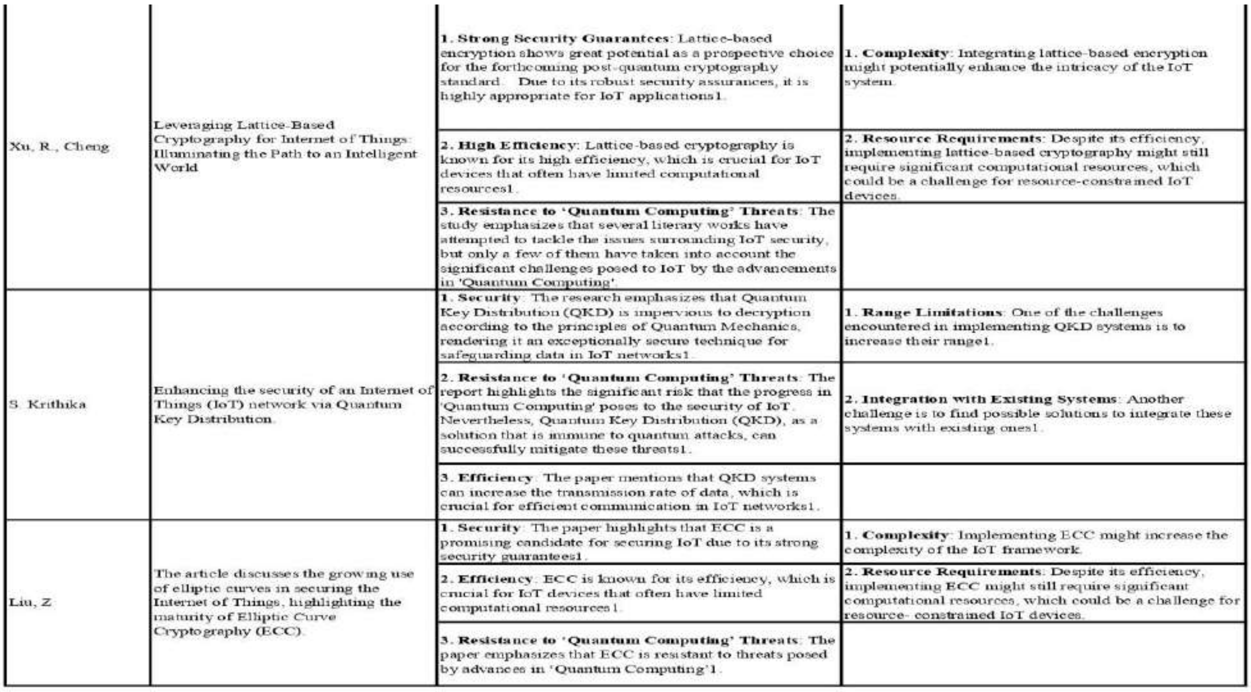
The authors examined the impact of 'Quantum Computing' on 'Cybersecurity', specifically upon widely employed cryptographic techniques. They then put forth recommendations for developing stronger cryptography algorithms that can withstand the computational capacity of both classical and Quantum Computers. In the end, they projected and implemented a 'Quantum-Resistant Algorithm' that was especially tailored for IoT devices, considering their constrained resources. In the end, a 'Quantum-Resistant Cryptographic System' for 'IoT' devices was effectively implemented. However, there are still other obstacles that must be overcome for IoT technology to effectively harness the power of 'Quantum Computing'. The authors of the paper Xu, R., et al. [6] introduced the notion of data safety and discussed the consequences of utilizing a 'Quantum Processor'. They propose employing a 'Lattice-based Methodology' for 'IoT' devices to protect against the capabilities of 'Quantum Computing'.

They then conducted an in-depth analysis of the most sophisticated applications of the 'Lattice-based Algorithm' on devices that have partial resources, such as 'IoT' devices. The study was performed at an advanced level, with a specific focus on the 'Lattice-based' approach. In summary, perspectives are shaped by current conditions and future discoveries about the use of the stated algorithm in 'IoT' systems. The figure 1 depicts the several uses of the 'Internet of Things (IoT)'. Gill et al. [5] assert that 'Quantum Advantage' can be utilized in many domains, including Medical, 'Cybersecurity', 'IoT', Meteorology, and National Laboratories, to tackle intricate matters like autonomous vehicles. The research undertaken by Hassija et al. [12] investigates the possible application of quantum technologies in next communication systems. In addition, they discussed other quantum techniques, such as, amplitude estimation unstructured search, cryptography, and quantum annealing.

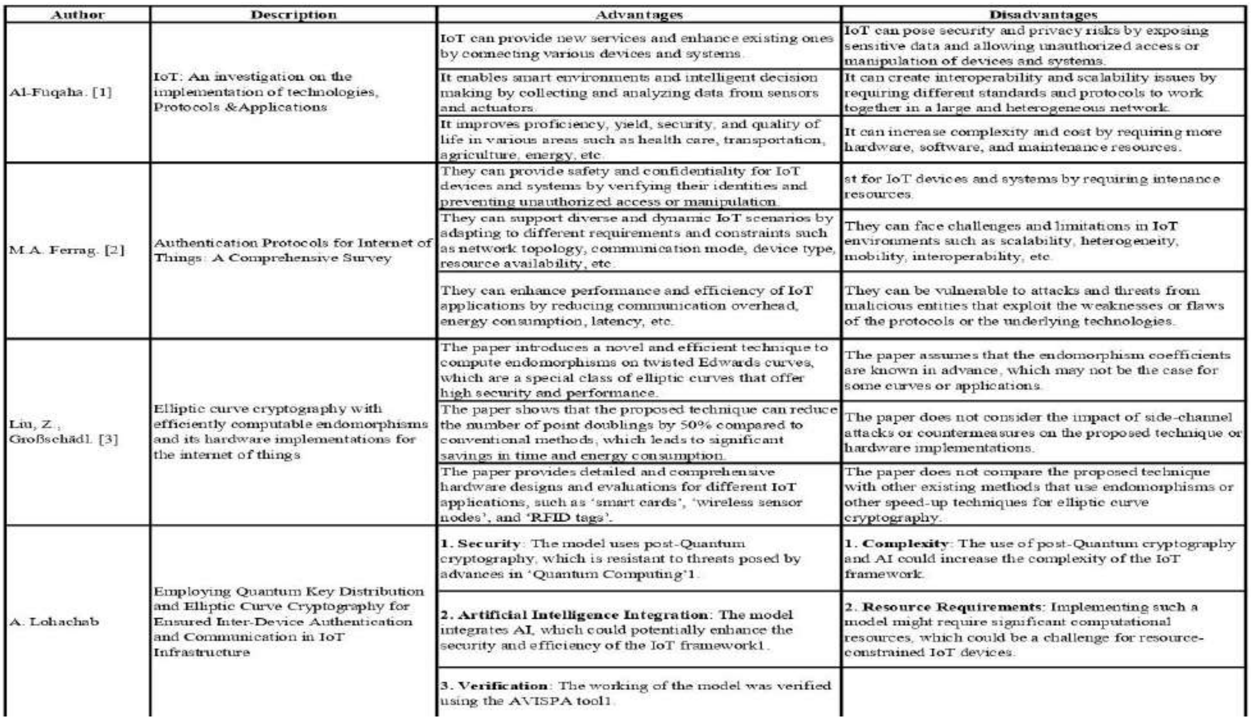
ISSN: 2583-7354

Table 1: Author work on quantum-enabled IoT security

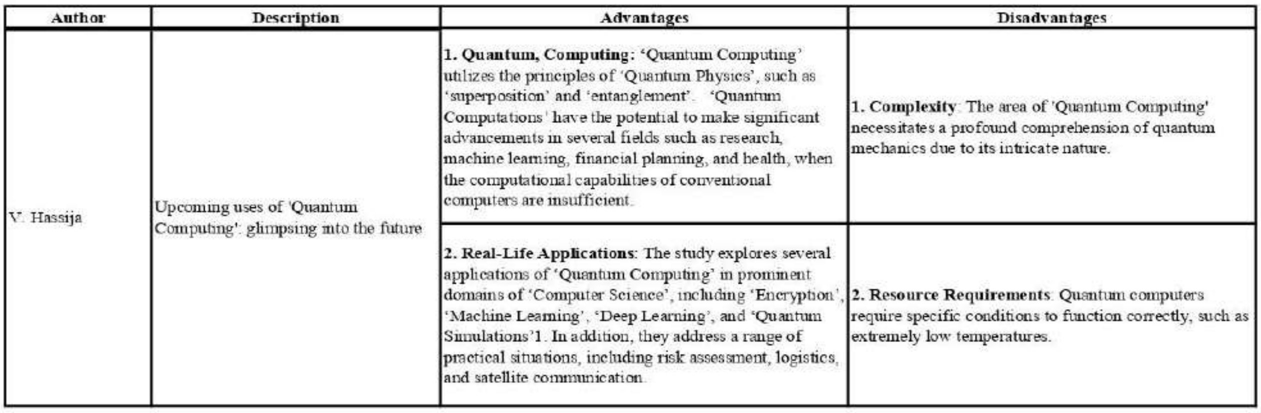




Author	Description	Advantages	Disadvantages
El-Latif	A robust quantum steganography protocol designed for the secure transmission of data in fog cloud-based IoT networks.	**1. Security**: The research emphasizes that the projected 'quantum steganography protocol' is resistant to well recognized attacks, including message, 'man-in-the-middle', and 'no-message attacks1'.	**1. Complexity**: Implementing quantum steganography might increase the complexity of the IoT framework.
		2. Authentication: The study presents a new quantum steganography algorithm that relies on a 'hash function' and 'quantum entangled states'. The 'hash function' is employed to verify the authenticity of embedded covert communications.	**2. Resource Requirements**: Despite its efficiency, implementing quantum steganography might still require significant computational resources, which could be a challenge for resource-constrained IoT devices.
		3. Efficiency: The suggested protocol does not utilize any extra communication channels other from the designated one for transmitting a confidential message or verifying security.	
M.S. Farash	A very effective user authentication and key agreement technique has been developed specifically for a heterogeneous wireless sensor network designed for the Internet of Things environment. This scheme is specifically built for Ad Hoc Networks.	**1. Efficiency**: The recommended method is very efficient, making it well-suited for IoT devices with limited resources.	**1. Complexity**: Implementing such a scheme might increase the complexity of the IoT framework.
		2. User Authentication: The system enables users to directly authenticate with a specific 'sensor node' in a diverse 'wireless sensor network'. This obviates the necessity of communicating with the gateway node2.	**2. Resource Requirements**: Despite its efficiency, implementing such a scheme might still require significant 'computational resources', which could be a challenge for resource-constrained 'IoT' devices.
		3. Key Agreement: The scheme includes a key agreement component, which is crucial for secure communication1.	
Cheng, C	Ensuring the security of the Internet of Things in a quantum computing era.	**1. Security**: The paper highlights that we currently trust the 'cryptographic algorithms' such as 'elliptic curve cryptosystems (ECCs)' as basic building blocks to secure the communication in the 'IoT'1. However, public key schemes like 'ECC' can easily be broken by the upcoming 'quantum computers'1.	**1. Complexity**: Implementing quantum- resistant cryptosystems might increase the complexity of the IoT framework.
		2. Quantum-Resistant Cryptosystems: The study specifically examines cryptosystems that are resistant to quantum attacks in order to secure the 'Internet of Things (IoT)'. This paper showcases the effects of 'Quantum Computers' on the security of current cryptographic systems, followed by an outline of recommended cryptographic algorithms that can withstand assaults from both classical and quantum computers1.	**2. Resource Requirements**: Despite their efficiency, implementing quantum-resistant cryptosystems might still require significant computational resources, which could be a challenge for resource-constrained IoT devices.
		3. Implementations on Constrained Devices: The paper discusses the current applications of 'Quantum-Resistant Cryptographic Methods' on limited devices that are appropriate for the 'Internet of Things (IoT)'.	
Xu, R., Cheng	Leveraging Lattice-Based Cryptography for Internet of Things: Illuminating the Path to an Intelligent World	**1. Strong Security Guarantees**: Lattice-based encryption shows great potential as a prospective choice for the forthcoming post-quantum cryptography standard. Due to its robust security assurances, it is highly appropriate for IoT applications1.	**1. Complexity**: Integrating lattice-based encryption might potentially enhance the intricacy of the IoT system.
		2. High Efficiency: Lattice-based cryptography is known for its high efficiency, which is crucial for IoT devices that often have limited computational resources1.	**2. Resource Requirements**: Despite its efficiency, implementing lattice-based cryptography might still require significant computational resources, which could be a challenge for resource-constrained IoT devices.
		3. Resistance to 'Quantum Computing' Threats: The study emphasizes that several literary works have attempted to tackle the issues surrounding IoT security, but only a few of them have taken into account the significant challenges posed to IoT by the advancements in 'Quantum Computing'.	
S. Krithika	Enhancing the security of an Internet of Things (IoT) network via Quantum Key Distribution.	**1. Security**: The research emphasizes that Quantum Key Distribution (QKD) is impervious to decryption according to the principles of Quantum Mechanics, rendering it an exceptionally secure technique for safeguarding data in IoT networks1.	**1. Range Limitations**: One of the challenges encountered in implementing QKD systems is to increase their range1.
		2. Resistance to 'Quantum Computing' Threats: The report highlights the significant risk that the progress in 'Quantum Computing' poses to the security of IoT. Nevertheless, Quantum Key Distribution (QKD), as a solution that is immune to quantum attacks, can successfully mitigate these threats1.	**2. Integration with Existing Systems**: Another challenge is to find possible solutions to integrate these systems with existing ones1.
		3. Efficiency: The paper mentions that QKD systems can increase the transmission rate of data, which is crucial for efficient communication in IoT networks1.	
Liu, Z	The article discusses the growing use of elliptic curves in securing the Internet of Things, highlighting the maturity of Elliptic Curve Cryptography (ECC).	**1. Security**: The paper highlights that ECC is a promising candidate for securing IoT due to its strong security guarantees1.	**1. Complexity**: Implementing ECC might increase the complexity of the IoT framework.
		2. Efficiency: ECC is known for its efficiency, which is crucial for IoT devices that often have limited computational resources1.	**2. Resource Requirements**: Despite its efficiency, implementing ECC might still require significant computational resources, which could be a challenge for resource- constrained IoT devices.
		3. Resistance to 'Quantum Computing' Threats: The paper emphasizes that ECC is resistant to threats posed by advances in 'Quantum Computing'1.	



Author	Description	Advantages	Disadvantages
Al-Fuqaha. [1]	IoT: An investigation on the implementation of technologies, Protocols &Applications	IoT can provide new services and enhance existing ones by connecting various devices and systems.	IoT can pose security and privacy risks by exposing sensitive data and allowing unauthorized access or manipulation of devices and systems.
		It enables smart environments and intelligent decision making by collecting and analyzing data from sensors and actuators.	It can create interoperability and scalability issues by requiring different standards and protocols to work together in a large and heterogeneous network.
		It improves proficiency, yield, security, and quality of life in various areas such as health care, transportation, agriculture, energy, etc.	It can increase complexity and cost by requiring more hardware, software, and maintenance resources.
M.A. Ferrag. [2]	Authentication Protocols for Internet of Things: A Comprehensive Survey	They can provide safety and confidentiality for IoT devices and systems by verifying their identities and preventing unauthorized access or manipulation.	st for IoT devices and systems by requiring intenance resources.
		They can support diverse and dynamic IoT scenarios by adapting to different requirements and constraints such as network topology, communication mode, device type, resource availability, etc.	They can face challenges and limitations in IoT environments such as scalability, heterogeneity, mobility, interoperability, etc.
		They can enhance performance and efficiency of IoT applications by reducing communication overhead, energy consumption, latency, etc.	They can be vulnerable to attacks and threats from malicious entities that exploit the weaknesses or flaws of the protocols or the underlying technologies.
Liu, Z., Großschädl. [3]	Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things	The paper introduces a novel and efficient technique to compute endomorphisms on twisted Edwards curves, which are a special class of elliptic curves that offer high security and performance.	The paper assumes that the endomorphism coefficients are known in advance, which may not be the case for some curves or applications.
		The paper shows that the proposed technique can reduce the number of point doublings by 50% compared to conventional methods, which leads to significant savings in time and energy consumption.	The paper does not consider the impact of side-channel attacks or countermeasures on the proposed technique or hardware implementations.
		The paper provides detailed and comprehensive hardware designs and evaluations for different IoT applications, such as 'smart cards', 'wireless sensor nodes', and 'RFID tags'.	The paper does not compare the proposed technique with other existing methods that use endomorphisms or other speed-up techniques for elliptic curve cryptography.
A. Lohachab	Employing Quantum Key Distribution and Elliptic Curve Cryptography for Ensured Inter-Device Authentication and Communication in IoT Infrastructure	**1. Security**: The model uses post-Quantum cryptography, which is resistant to threats posed by advances in 'Quantum Computing'1.	**1. Complexity**: The use of post-Quantum cryptography and AI could increase the complexity of the IoT framework.
		2. Artificial Intelligence Integration: The model integrates AI, which could potentially enhance the security and efficiency of the IoT framework1.	**2. Resource Requirements**: Implementing such a model might require significant computational resources, which could be a challenge for resource-constrained IoT devices.
		3. Verification: The working of the model was verified using the AVISPA tool1.	



Author	Description	Advantages	Disadvantages
V. Hassija	Upcoming uses of 'Quantum Computing': glimpsing into the future	**1. Quantum, Computing**: 'Quantum Computing' utilizes the principles of 'Quantum Physics', such as 'superposition' and 'entanglement'. 'Quantum Computations' have the potential to make significant advancements in several fields such as research, machine learning, financial planning, and health, when the computational capabilities of conventional computers are insufficient.	**1. Complexity**: The area of 'Quantum Computing' necessitates a profound comprehension of quantum mechanics due to its intricate nature.
		2. Real-Life Applications: The study explores several applications of 'Quantum Computing' in prominent domains of 'Computer Science', including 'Encryption', 'Machine Learning', 'Deep Learning', and 'Quantum Simulations'1. In addition, they address a range of practical situations, including risk assessment, logistics, and satellite communication.	**2. Resource Requirements**: Quantum computers require specific conditions to function correctly, such as extremely low temperatures.

3. SECURITY ISSUES IN IOT

The progress of 'IoT-enabled communication' has been facilitated by the implementation of cutting-edge technologies in several fields, like smart agriculture, creative health care and intelligent cities. The 'Internet of Things (IoT)' devices that offer these applications transmit vast volumes of data across many contexts. The proliferation of 'IoT' applications leads to a rise in 'cyber-attacks'. Moreover, it poses potential threats to the confidentiality and privacy of users. The main security concerns associated with the 'IoT' ecosystem are verification, authorization, integrity, and trust management. Figure 2 illustrates the presence of notable security concerns within the layered structure of IoT. This section analyzes the possible hazards to the structure of the IoT and the benefits of integrating the 'Quantum Layer' to bolster 'IoT' security.

'Sensing Layer'

This layer incorporates a range of sensing technologies, including WSN, RFID, and GPS, to facilitate IoT applications. Each of these technologies plays a role in the administration of IoT actuators and sensors. Sensors are utilized to detect info from the surroundings, including ultrasonic, video, and temperature sensing. The sensing layer is susceptible to several forms of assaults, such as sensor node capture, insertion of counterfeit data codes, 'eavesdropping', and 'sleep deprivation attacks'.

'Network Layer'

'Computational Units' are necessary to process the data received from the bottom layer, notably the 'Sensor Layer'. The main function of the Network Layer is to convey the data acquired from the 'Sensor Layer' to the processing units. Processed data is essential for enabling 'IoT' applications. However, the unrestricted internet connectivity exposes ‘Network Layers’ to substantial security vulnerabilities, such as access control attacks, Denial of ‘Service attacks’, and attacks through data transfer.

‘Quantum Layer’

The ‘Quantum Layer’ provides strong security safeguards for ‘Internet of Things (IoT)’ applications. It involves the safe transmission of cryptographic keys. At this level, the confidentiality and integrity of keys are guaranteed by the principles of quantum mechanics. However, this layer enabled the adoption of ‘Quantum-Based Encryption’, which is vulnerable to security threats such as ‘individual’, ‘collective’, and ‘coherent assaults’.

‘Application Layer’

The ‘Application Layer’ is responsible for providing services to the user in order to support decision-making. The essential applications of the ‘Internet of Things (IoT)’ encompass smart cities, intelligent surroundings, efficient healthcare, and intelligent grids. Ensuring privacy, confidentiality, and data authentication poses substantial issues in the utilization of IoT across many applications. The main considerations at the ‘Application Layer’ are ‘eavesdropping vulnerabilities’, ‘access control measures’, ‘service interruption attacks’, and ‘malicious code intrusions’.

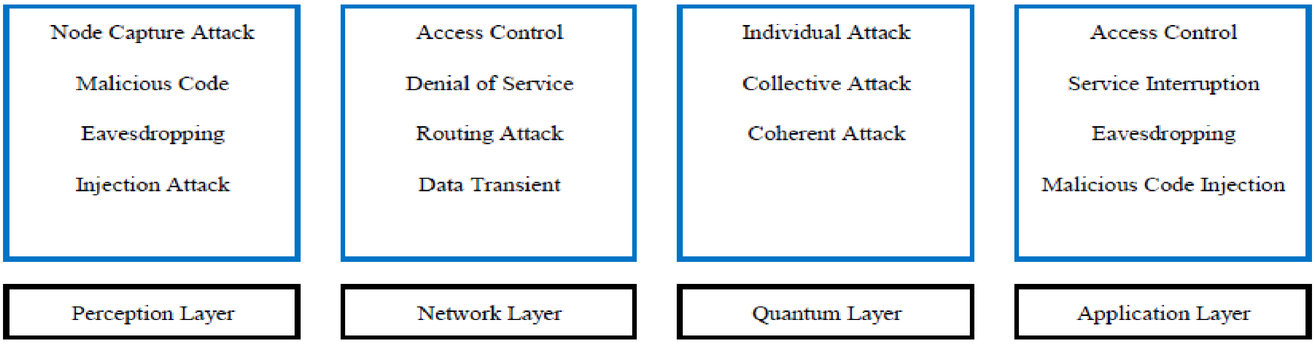


Figure 2: Layered ‘IoT’ Architecture

4. INCIDENTS OF CYBER INTRUSIONS TARGETING INTERNET OF THINGS (IOT) NETWORKS

While IoT-enabled networks offer significant flexibility and precise control over various processes and services, these apparent advantages are regrettably accompanied by significant security vulnerabilities. As a vast number of smart devices with modest capabilities and low energy usage are connected in a distributed network, conventional security measures and boundaries are no longer effective [13][14][15]. The estimated quantity of interconnected devices and allocation of security expenditure are illustrated in Figure 3.

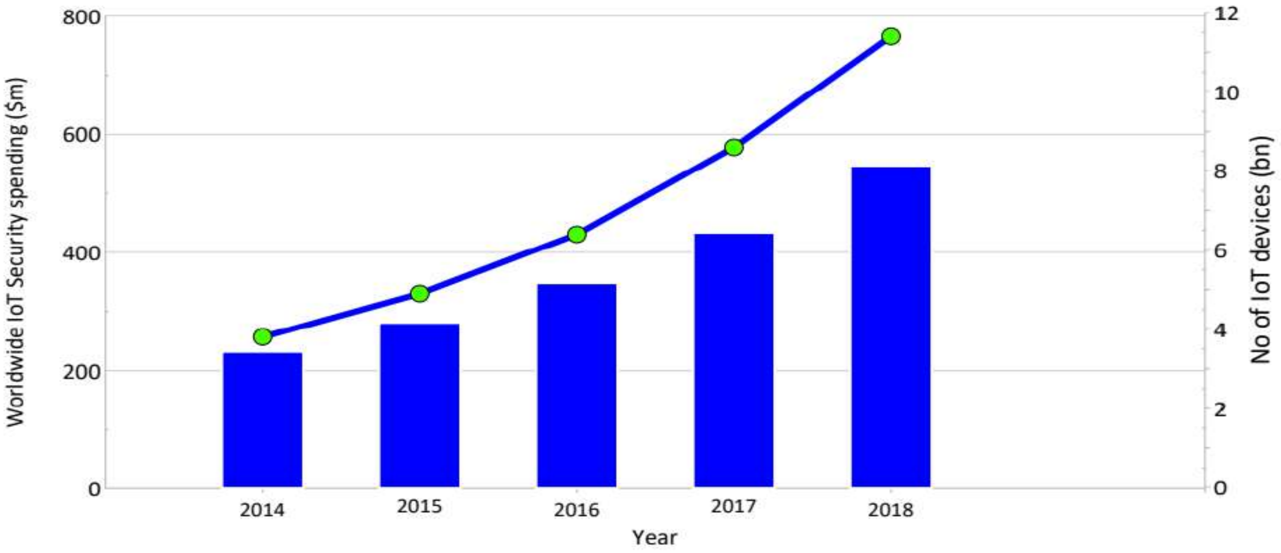


Figure 3: A projection: Number of connected devices and security budget

The abundance of vulnerabilities in IoT devices provides cyber-criminals with opportunities to target IoT networks. The IP cameras, printers, and routers' vulnerabilities were exploited to initiate Mirai botnet attacks [14]. Figure 4 displays the most recent facts on IoT attacks.

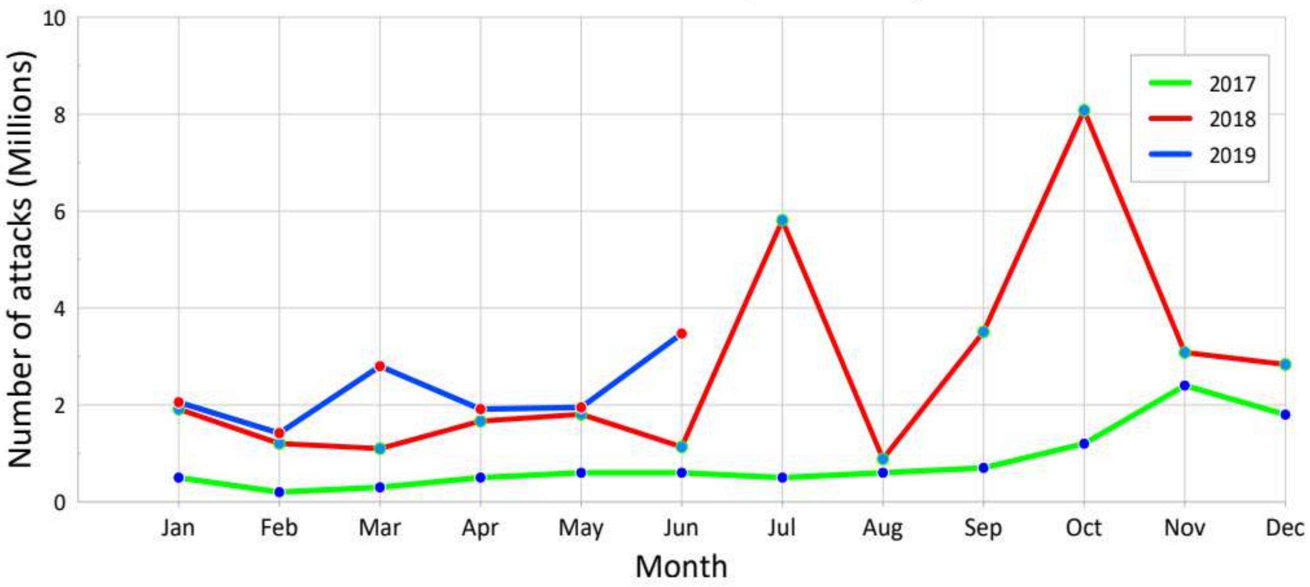


Figure 4: Recent IoT attack statistics

Below is a concise overview of the characteristics of several IoT applications that make them susceptible to assaults. The fundamental infrastructure of any automated enterprise is the Industrial Control System (ICS), which encompasses Supervisory Control and Data Acquisition (SCADA) networks and Programmable Logic Controllers (PLC). The substitution of traditional electro-mechanical control systems with embedded electronics has provided appealing opportunities for cyber-fraudsters. The integration of IP-connected devices into industrial automation systems to achieve IoT systems has created more chances for attackers.

Attackers are currently attempting to breach networks by taking advantage of the vulnerabilities present in IoT devices, as traditional networks have robust defensive measures in place. There is a need for more inquiry into the security problems of IoT-based services due to the growing number of attacks. Additionally, better defense mechanisms should be implemented to protect the current Internet of "insecure" Things.

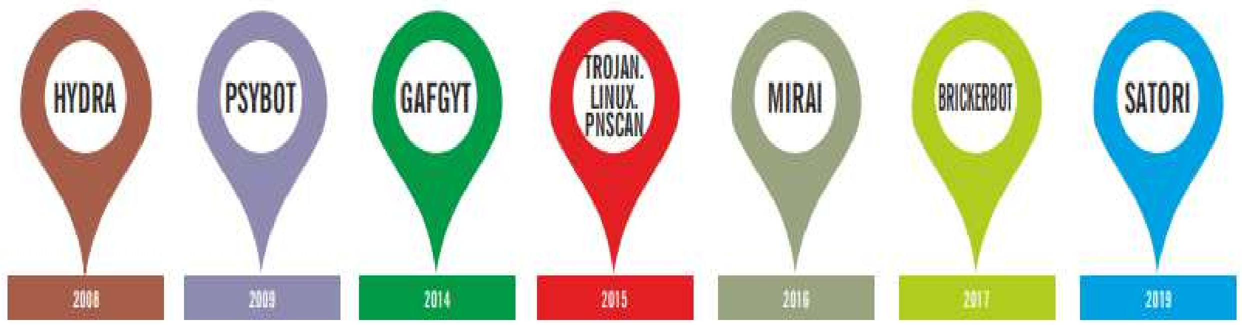


Figure 5 displays a chronological sequence of significant IoT attacks

‘Quantum – enabled Internet of Things (IoT)’

An ‘IoT’ framework is a network of interconnected devices utilizing diverse technologies such as ‘Wi-Fi, Bluetooth, Zigbee, Bluetooth, and 6LOWPAN’. These technologies facilitate the advancement of the Internet of Things (IoT). These technologies facilitate the transmission of data in ‘Internet of Things (IoT)’ applications, including smart cities, advanced medical infrastructure, and intelligent farming. The integration of IoT with ‘Quantum Computing’ is crucial for ensuring data privacy and secrecy in these applications. The existing safeguarding of the IoT communication infrastructure relies on conventional cryptographic techniques, including the use of Public and Private-key structures. However, these methods are vulnerable to attacks from quantum computers. Theoretical vulnerabilities in public-key infrastructure have previously been uncovered through the advancement of ‘quantum algorithms’ like as ‘Shor's’ and ‘Grover's’.

Securing sensitive information in IoT connectivity is important owing to the constrained resources of the devices involved. Therefore, it is crucial to implement safe and lightweight encryption. Moreover, the need to tackle both conventional and quantum threats provide an opportunity for the advancement of quantum-resistant cryptography [7]. 'Quantum computing' will be important for making sure safe contact in the ‘Internet of Things (IoT)’ in the future. Researchers have looked at a number of ‘Quantum-Based Methods’, and Figure 3 shows a comparison of them.

5. DIFFICULTIES ASSOCIATED WITH QUANTUM-BASED INTERNET OF THINGS (IOT)

- ‘Quantum Key Distribution’: It provides a dependable means of sending cryptographic keys. Assuming, however, that the identification of an unauthorized listener on the ‘quantum communication’ channel took place. Under such circumstances, the entire procedure is invalidated, and further communication will not commence until any interception of information is completely absent from the channel.
- ‘Communication over a limited physical distance’: Mass communication among Internet of Things (IoT) users using the quantum channel is challenging because Quantum Key Distribution (QKD) has a restricted range for communicating over short distances.
- ‘Quantum Reversible Computing’: The existence of eve presents a severe danger to quantum-based reversible computation [28].
- ‘Cybersecurity Breach’: Quantum-based communication can be targeted by specific attacks. In this scenario, the attacker creates a new ‘quantum channel’ by intercepting a ‘quantum signal’ that is being transferred between Alice and Bob.

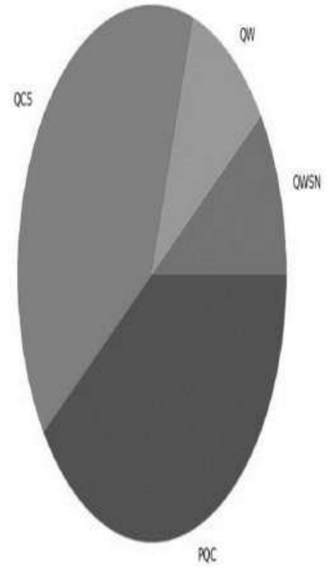


Figure 3: Examine quantum-based methods including ‘Quantum Computing methods (QCS)’, ‘Post Quantum Cryptography (PQC)’, ‘Quantum Wireless Sensor Networks’ and ‘Quantum Walk (QW)’.

6. CONCLUSION

Based on the preceding section, it can be inferred that scholars have conducted studies in several domains utilizing a range of techniques and algorithms. The researchers presented keyaspects pertaining to the assessment of their proposed methodologies. The IoT is the interconnectedness of various devices, allowing them to communicate with one other. This connection offers several benefits to customers by simplifying decision-making processes. It is imperative that such technology, which encompasses vital informationin areas such as healthcare, smart cities, and military applications, is fortified with robust security measures. There are several traditional cryptographic primitives that guarantee secure communication by depending on ‘complex mathematical structures’. The security offered by ‘traditional cryptographic architecture’ is no longer dependable due to its susceptibility to 'Quantum Computing' assaults. Hence, connectivity provided by IoT necessitates the implementation of quantum-based security measures in order to withstand potential quantum attacks in the future.Our survey focused on examining quantum-based cryptographic protocols designed to enhance the security of IoT connectivity. This article provides a thorough analysis of ‘security attacks’ on ‘Internet of Things (IoT)’ applications. The paper explores strategies that can resist quantum assaults in order to safeguard IoT communication, quantum authentication techniques, quantum key distribution (QKD), and the difficulties encountered in deploying quantum-enabled IoT communication. Therefore, this work provides significant suggestions for future 'IoT' researchers to include 'quantum-resistant technologies'.

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M.: 'Internet of things: A survey on enabling technologies, protocols, and applications', IEEE CommunicationsSurveys & Tutorials, 2015, 17, (4), pp. 2347-2376

[2] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, L. Shu, Authentication Protocols for Internet of Things: A Comprehensive Survey, Secur. Commun. Networks. 2017 (2017). https://doi.org/10.1155/2017/6562953.

[3] Liu, Z., Großschädl, J., Hu, Z., Järvinen, K., Wang, H., and Verbauwhede, I.: 'Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things', IEEE Transactions o6n Computers, 2017, 66, (5), pp. 773-785

[4] Lohachab, Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure, SSRN Electron. J. (2018). https://doi.org/10.2139/ssrn.3166511

[5] S.S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, R. Buyya, 'Quantum Computing': A taxonomy, systematic review and future directions, Softw. - Pract. Exp. 52 (2022) 66–114. https://doi.org/10.1002/spe.3039.

[6] Xu, R., Cheng, C., Qin, Y., and Jiang, T.: 'Lighting the Way to a Smart World: Lattice-Based Cryptography for Internet of Things', arXiv preprint arXiv:1805.04880, 2018

[7] S. Krithika, T. Kesavmurthy, Securing IOT network through quantum key distribution, Int. J. Innov.Technol.Explor.Eng.8(2019)693–696. https://doi.org/10.35940/ijitee.F1141.0486S419.

[8] Liu, Z., Huang, X., Hu, Z., Khan, M.K., Seo, H., and Zhou, L.: 'On emerging family of elliptic curves to secure internet of things: ECC comes of age', IEEE Transactions on Dependable and Secure Computing, 2017, 14, (3), pp. 237-248

[9] El-Latif, A.A.A., Abd-El-Atty, B., Hossain, M.S., Elmougy, S., and Ghoneim, A.: 'Securequantum steganography protocol for fog cloud Internet of Things', IEEE Access, 2018, 6, pp.10332-10340

[10] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks. 36 (2016) 152–176. https://doi.org/10.1016/j.adhoc.2015.05.014 .

[11] Cheng, C., Lu, R., Petzoldt, A., and Takagi, T.: 'Securing the Internet of Things in a quantum world', IEEE Communications Magazine, 2017, 55, (2), pp. 116-120

[12] V. Hassija, V. Chamola, A. Goyal, S.S. Kanhere, N. Guizani, Forthcoming applications of 'Quantum Computing' : peeking into the future, 1 (2020) 35–41. https://doi.org/10.1049/iet- qtc.2020.0026.

[13] Frustaci, Pace, Aloi, and Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, 2018.

[14] Kolias, Kambourakis, Stavrou, and Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.

[15] Yang, Wu, Yin, Li, and Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[16] SonicWall 2019 Mid-Year Threat Report. [Online]. Available: https://i.crn.com/ sites/default/files/ ckfinderimages/userfiles/ images/crn/custom/2019/SonicWall. Accessed: 17-10-2019.

Cite this article as: Dr. Kirti Diddi et al. (2023). A Survey on 'Quantum Computing' Applications to Bolster Security in the "Internet of Things (IoT)'. International Journal of Emerging Knowledge Studies. 2(12), pp. 807-815.