International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

Review on Quantum Methods to Measure the Performance, Security, And Privacy for the Iot Framework

Siva Hari Naga Shashank Varagani
Independent Researcher, Staff Software Engineer
Florida, USA.
sivanagv12@gmail.com

Abstract: Millions of devices worldwide, including smart appliances for domestic use such as smart TVs, thermostats, and CCTV cameras, were connected by the evolution of the internet. It was allowing the entire human community to connect and access devices from all over the globe through cloud infrastructure. Increasing IoT devices weaken classical model computing performance, making the IoT framework a failure model. Another big problem for IoT devices is keeping personal information safe and private because attackers can get in while the devices are talking to each other. The safety measures we have now, like changing passwords often, keeping IoT devices up to date, using a backup network (VPN), and not using plug-and-play features, work up to a point but can't promise that everything is 100% safe. Because of new technology, the public key cryptography method (RSA), which is thought to be safe right now, is being used more and more. One Time Pad (OTP) is thought to be a good way to encrypt information securely in classical cryptography, but it takes too long to send the key between parties. The trade-off between adding more IoT devices and traditional security methods isn't fair, so we needed a new technology to fix the issue. Modern innovations called quantum computing is being developed. This will help find long-term solutions for the speed and security problems that affect millions of IoT devices. Quantum technology operates on the principles of quantum physics, as opposed to existing technology, which is based on conventional physics. While classical cryptography utilizes deterministic bits that can be hacked, quantum cryptography uses qubits, which are superpositions of 0 and 1. The measurement of an unknown qubit, which provides ½ probabilities of measuring in either bit '0' or bit '1', complicates the prediction of the data. Grover's algorithm searches an unsorted databases in O(√n), as opposed to O(n) in classical algorithms, and Shor's algorithm in quantum computing solves factoring a huge integer in polynomial time, compared to quadratic time in conventional models. The privacy problem and the need for high-level security can be addressed by applying the laws underlying quantum physics and such as the Heisenberg principle and the no-cloning theorem, to detect when an unauthorized user is involved in a current connection. Heisenberg's uncertainty principle says that you can't measure quanta that aren't known without upsetting them, which means that a third party has to be involved. It is impossible to create a copy of the unknown states due to another quantum characteristic called the No-cloning theorem. Therefore, an enemy cannot copy the quantum state in order to read the quantum information in safe communication. Communication in quantum computing can also happen through entanglement, in which a third party creates an entangled photon and sends a qubit to the parties talking to each other. If one party measures a qubit, it will match up with measurements made by the other party. This creates a safe key. When two parties communicate directly and securely without the use of a key, it's known as quantum secure interacting directly, or QSDC. Quantum and conventional security should be combined for high-level IoT security.

Keywords: Quantum, IoT Devices, Quantum bits, Cryptography, probability.

I. INTRODUCTION

People in the 21st century depend on technology for everything they do, like doing business or talking to their home appliances like TVs, thermostats, and CCTV cameras wirelessly over the internet[1]. The global population is 7.8 billion (2021 population survey), and 3.8 billion people utilize smart phones and digital household utilities (about 7–8 devices per user) for daily tasks [2,3]. The parent want to raise a child at home while carrying out official duties in a workplace setting, and they can accomplish this by using smart devices that are readily available on both ends. Parents may use closed-circuit television cameras to verify the identity of visitors before deciding whether to let them inside their home or not. All household devices consist of sensors and actuators that are connected at the initial stage of the

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

Internet of Things (IoT) architecture. An internet gateway, such as Wifi or wired LAN, gathers data from sensors and compresses it to an appropriate size before further processing it in an EDGE enabled system. Third stage: capturing data and sending it to a remote site at the same time [4]. The final phase of the process involves storing the data for in-depth examination and conducting predictive analysis. IoT devices and their features are relied upon by parents to keep an eye on their children, so the processing speeds of all of them should be reliable so that there are no delays or problems in the connection between them. All gadgets are networked together to create an Internet of Things, or Internet of gadgets (IoT), which facilitates efficient communication between them but slows down computation when using traditional techniques.

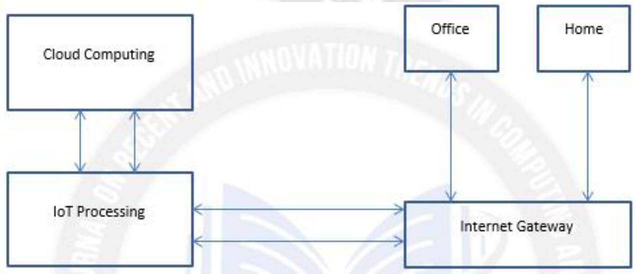

Figure 1. IoT Architecture

According to Gorden Moore, the number of transistors on Integrated Circuits (ICs) wills double every two years, resulting in greater processing speed due to the use of smaller ICs [5]. The validity of Moore's Law is approaching obsolescence in the present period, thereby making it impossible to achieve quicker device computability by reducing the integrated circuits (ICs) [6]. Further increasing the transistor count in an integrated chip is not possible; thus, the compute capability of an IoT device will not expand, resulting in the failure of the IoT paradigm. Because the computational mechanism of the classical model follows a sequential pattern, machine learning or prediction algorithms will execute slowly and cause delays. An advanced technology is necessary to enhance the computational complexity, enabling effective implementation of the IoT model and real-time service without any delay as represented in Figure 1.

Eleven point one point two enhancing computational efficiency via quantum technology. When considering computer technologies, the evolution of quantum mechanics has brought about a significant transformation from conventional approaches. Classical computers store information using classical bits, which can be either '0' or '1'. In contrast, quantum computers use qubits for computation. A decimal number chosen from the set {0,1,2,3} can be represented by two classical bits, specifically {00,01,10,11}. Convert the decimal number '0' to the number '3', where the first classical bit is '0' and the second bit is also '0'. This computation requires two consecutive operations to be carried out. In traditional computing with 'n' bits, only one bit can be modified at any given moment, despite the reason that there are 2n potential combinations that can occur. In the field of quantum computing, a qubit has led to capacity to exist in a pure state. Hadmard gate moves it to a superposition state where it can be in the two states "0" or "1" at the same time. This makes it faster to compute than the old way [7]. The proposed it can be represented in stacked state for a two-qubit system. The four sequences {00, 01, 10, 11} can be represented parallel based on probability as in Figure 2.

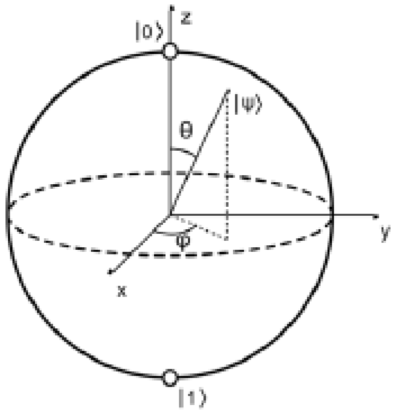

Figure 2. Quantum Sphere

The One Time Pad (OTP), also known as Vernam cipher [9], generates and corresponds a secret password between two parties in an anonymous way under certain conditions. Key Length compared to message Length; The key may be utilized only once; its recurrent use may result in the disclosure of sensitive information; There is a private exchange of keys between two people. Current key exchange protocols rely on the Diffie-Hellman Key Exchange algorithm, which is thought to be secure for surreptitiously passing keys between parties; but, with the advent of dimension hacking, novel ways of utilizing quantum technology are required.

Thus, we have developed the following main research question (MQ):

What is the main research projects involving quantum computing applied to routing problems carried out throughout the entire twenty-first century?

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

Which is the field being studied's temporal progression?: What are the primary routing issues that the researchers encounter?: Which types of studies—theoretical or applied—do authors favors the most?: What kind of algorithmic schemes are most commonly utilized?: What is the quantum computer that is used the most?: Which are the field's most cited papers?: Which writers, organizations, and geographical areas are the most prolific?: What are the community's primary predictions for future challenges?

II. REVERSIBLE VS. IRREVERSIBLE CIRCUIT: QUANTUM PARALLELISM

All aspects of classical computing, with only one exception of operation, are irreversible in execution. In classical computing, if we offer two inputs in an AND gate and get a single output state, we can't tell which input states were used to process the output. In classical physics, when an operation is conducted on two inputs and yields one output, heat energy is lost during the procedure, leaving insufficient heat energy to do the reverse action. In Quantum computing, the quantum circuits are implemented in a removable manner, utilising an auxiliary bit to store the current computed value and ensuring that the original input variables are not lost [10]. Quantum circuits exhibit reversibility when subjected to unitary transformations, but once measured; this reversibility is lost and cannot be restored.

Consider an XOR gate and execute it in both classical and quantum circuits. The XOR gate produces an output of '1' when the input bits are different and an output of '0' when the input bits are the same. In a classical circuit with only one output, two input bits can't be made. But in a quantum circuit, we keep the original input bit and use the XOR calculation to turn the process around. The construction of efficient quantum circuits necessitates the involvement of numerous unitary operation gates and ancillary bits. The greatest number of ancillary bits required to construct 'n' bit input bits is 'n-1' auxiliary bits. The overall design for successfully transforming a classical circuit into a quantum circuit [11].

A. GROVER ALGORITHM:

Grover's Algorithm, a quantum search technique, enhances the searching approach in O(√N) compared to the best classical algorithm, O(N). Classically, searching things is required alongside Include items to determine found or not found. Grover's search relies on how many times Oracle (Grover's Iteration) was called to determine if an element is included in a list or not. Let's illustrate this with an example: Given a list of numbers from 0 to N-1, where each number is either marked as 0 (not found) or 1 (found), with the condition that only one number is marked. The grover's algorithms began with superposition state. First, apply the uniform transformation upon states. To discover the average or inversion mean of all the elements, flip the sign of the element that is being searched (x*). Just like a data scientist, you'll notice that the amplitude of the searched element increases while the inversion means average freezes after a few iterations. This is why the number of Grover's iterations determines the complexity of Grover's search.

B. QUANTUM PROPERTIES TO FACILITATE COMMUNICATION:

In the previous conversation, we explored the challenges faced by the modern era in ensuring the secure transmission of information between two parties. Let's now examine how the characteristics of quantum technology enable us to guarantee complete security throughout the exchange of messages between participants in an incident whenever a third party is involved.

i. Principles of Heisenberg:

In quantum mechanics, Heisenberg's principle asserts that when an item travels through space, its velocity and position cannot be measured correctly at the same time; this approach is used in conveying quantum information over a communication channel. Although expressed as an equation, the Heisenberg uncertainty principle is represented as Planck's constant (1). The equation $\Delta v \ \Delta p \geq h/4\pi$ represents a fundamental principle in physics, where h represents Planck's constant [15]. During a transfer of an unknown qubit between two parties, if an adversary tries to measure it, the qubit changes to a pure state, making it hard to get it back to the unknown form it was sent in. There will be a mismatch between the sender and recipient qubits once an adversary enters the transmission. The mismatch will result outside an announcement of unknown parties' engagement in communication, which will cause both message parties that communicate to cancel their present transmission.

Let's consider an example where Alice generates an unknown qubit state and sends it to Bob. There is an unknown adversary (EVE) who interferes with communication by manipulating the quantum channels. They do this by measuring the qubit sent by Alice, preparing a new state, and then sending it to Bob for measurement. After communicating in quantum channel, Alice and Bob will communicate on Authenticate public channel to test trustworthiness. If Alice and Bob realize that the sent qubit doesn't match Bob's qubit, they will terminate the current transmission.

Another critical property of quantum mechanics is entanglement. When two qubits are maximally entangled or mixed, the measurement of one qubit is correlated with another. To illustrate, let's say that the first qubit is |0>, and the second qubit is |1>. Applying a hadamard (H) and identity transformation on the first 1/(√2) (|0>+|1>) and second qubit (I) yields the unentangled state 1/(√2) (|01>+|11>). Now, use the CNOT transformation on the first qubit, which serves as the control qubit, and another qubit, which serves as the target bit, to achieve an entangled state of 1/(√2) (|01>+|11>). The four possible entangled states come from a Bell state change [16]. They are <|0>|0>,|0>|1>,|1>|0>,|1>|1>.Transferring the unknown qubit with two classical bits leads to teleportation [17] and super dense coding [18] in quantum communication.
No Coding Theorem: The primary drawback of classical cryptography is the bit's duplicability, which allows for the copying and sending of cipher text to the recipient. Afterwards, the cypher can be decrypted to reveal the information concealed within the encrypted text. There is no way to copy as well as clone undefined quantum states, according to the No. cloning theory [19]. Considering an unknown state, let's say that |c>= 1/(√2) (|a>+|b>), the adversary want to apply an artificial bit (|0>) to clone the unknown bit using a unitary transformation. U. U(|c>|0>)=1/√2((U|a>|0)>+U(|b>|0>)). Imagine a scenario where a unitary transformation is applied to a pure state. This transformation results in the state |a>|0> being transformed into |a>|a>, and the state |b>|0> being transformed into |b>|b>. as it is applied to the unknown state, we get U(|c>|0>)=1/√2((U|a>|a)>+U(|b>|b>)). The cloning process involves duplicating the state U(|c>|0>)=|c>|c> = 1/(√2) (|a>+|b>)1/(√2) (|a>+|b>) can be expressed as 1/2 (|a>|a>+|a>|b>+|b>|a>+|b>|b>), which means that it is impossible for any unitary operation to accurately duplicate or clone unknown quantum states.

III. QUANTUM SECURE DIRECT COMMUNICATION

The two-way protocol is a secure and bidirectional method of communication that allows both parties to exchange messages without the need for a key. Instead of allowing Alice and Bob to communicate directly, QSDC requires Alice to start the conversation, Bob to encrypt the message, and Alice to decrypt it in terms of measurement. Deterministic secure two-way communication, namely the Ping Pong protocol with entanglement [20] and without entanglement [21], explains the two distinct techniques.

The Ping Pong protocol consists of two steps:

Ping (Alice begins communication) and Pong (Bob responds to Alice by encoding or measuring).

As an illustration,

- Let’s say Alice generates an EPR pair in the entangled state φ+=1/√2(0H1T+1H0T), keeps the home qubit (H) in his lab, and sends the journey qubit (T) to Bob. Bob carries out two operations with a certain probability in control mode and a slightly lower probability in message mode.
- In Message mode, Bob will use unitary transformation (I or Z) on the journey bit to encode the classical bit '0'.
- Bob will perform the Identity transformation and, to encode a bit '1', he will perform the Z transformation.
- Identity transformation did not affect trip bit, although Z transformation transformed it to ‘-1’.
- Alice will execute measurement after receiving the journey bit from Bob and maintaining an entangled state.
- If Alice discovers that same state that was prepared, Bob will learn that the Bob bit is '0', and for different states, the Bob bit is '1'.
- The message mode is insecure since an adversary's involvement in communication cannot be recognized, and the full message can be disclosed to a third party.
- In control mode, the measurement of the transit bit is conducted in a computational basis that provides bits 0 or 1 with equal probability, rather than performing a gate operation.
- When the measurement is completed, the results will be transmitted to Alice via public authenticated channels.

- Please stop communicating at this time if Alice Bit and Bob are identical.

An opponent is likely to be involved. If Alice and Bob's bits are different, then the message that was sent is thought to be valid. Since the adversary does not exist in message mode, a control mode was needed to see if the adversary was involved in contact. Extension and modification of the ping pong protocol through the utilization of a super dense coding method developed by Bostrom and Felbinger [22], as well as the utilization of high-dimensional GHZ states in place of two the qubit states, in conjunction with quantum swapping [23-25].

Instead than relying on entanglement for secure direct connection, Lucamarini and Stefano Mancini [21] devised the orthogonal state to provide two-way protocol communications. The general structure of the protocol is similar to that of Ping Pong methods, except that it explicitly entangles the state and uses unentangled states for two-way communication.

For illustration purposes,

- Let’s say Alice generates a qubit in a computational or diagonal basis and sends it to Bob.
- Bob must conduct an operation depending on probability 'c' for message mode or probability 'c-1' for control mode.
- If Bob is in Message mode, he can encode bits 0 and 1 by using the unitary transformation of Identity and X (swap) and Z, respectively.
- In control mode, Bob will perform estimation in computational or diagonal bases and compare the results with Bob in classical mode to verify the presence of an intruder in communication.
- Alice's operation is dependent on Bob's mode selection probability.
- If Bob selects the Message mode, Alice will decode the information delivered by Bob.
- Alice must compare Bob's basis with her own and reject any that don't match if Bob selects the Control option.
- To verify the adversary's communication involvement, several samples are gathered on a matched basis.

Block transmission and order rearrangement techniques, in conjunction with one-time pad [26], have recently been developed to enable single-level systems to function as message carriers in communication processes [27]. Secret frequency-dependent phase modulation techniques are used to make deterministic secure communication practicable in today's environment [28].

The further development of techniques in QSDC leads to the creation of Quantum Dialogue, also known as bidirectional QSDC, in which Alice and Bob employ one of two QSDC rules to collaborate in a verified manner [29, 30].

IV. QUANTUM KEY DISTRIBUTION

The vernam cipher, also known as One Time Pad (OTP), is the safest modern security system. This is because quantum computing has become more advanced.

The fundamental disadvantage of OTP is key distribution between parties; while diffe-helman deems key exchange protocols to be safe, quantum data transfer is lacking. These days, we don't have enough current technology to improve security. We need either quantum encryption or post-quantum technology (based on math). We will talk about the Two Key distribution process BB84 [31] and Ekret B91 [32] below.

A. Scheme over BB84:

Charles Bennett and Gilles Brassard proposed the Heisenberg-based BB84 practice around 1984 for the quantum key distribution. The method is based on the idea of polarization in quantum physics and how quantum particles act when they are moved between two different bases.
In the BB84 protocol [31],

- Alice randomly generates ‘n’ classical bits and polarizes (computational or diagonal basis) using a quantum random number generator (QRNG)[33].
- When compared to the commonly used quasi random number generator, which creates unpredictability by following a pattern that can be predicted, QRNG truly generates random numbers.
- After being polarized with a random bit, the qubit will be sent to Bob through the quantum channel.
- Bob will then use QRNG to make the selection of Basis random.
- The selection of the same basis by Alice and Bob results in a likelihood of one hundred percent to produce the same classical bit, while the selection of another basis chosen by Alice results in an overall likelihood of fifty percent to produce the same basis.

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

- After quantum communication, there is classical communication.
- Alice and Bob will fix any mistakes so they can compare and hold on to the classical bit where the same base was chosen.
- Key shifting steps to verify Quantum Bit Error rate (QBER)[34] for intruders while comparing classical bits from both parties.
- Noise in the transmission channel or the presence of an intruder can cause QBER.
- If the QBER is higher than the threshold number, the current communication will end, and the process will start over until the raw is created.
- This results in the creation of a finite key that can be precisely utilized for purposes other than securing communication.
- Assuming Alice makes n=100, n will drop to 1/2 while fixing errors and another ½ will drop during the key moving process, leaving only ¼ of the key as a raw identifier.

1. Alice makes the five classical bits, polarizes them with photons, and sends them to Bob to be measured.
2. Bob sends Alice the measured basis, and Alice compares it.
3. The second and third bits that don't match are thrown away, but the first, fourth, and fifth bits that do match are kept for the key shift process.
4. In shifting, Alice's initial bit utilizes something comparable basis as Bob's circle, but her classical bit value varies, revealing Eve.
5. If a lot of bits are found to be different, either stop the protocol or do something to improve privacy.
6. Non-orthogonal bases were utilized for communication with minimal overhead [35].
7. Six state procedures [36, 37] with three non-orthogonal bases (X, Y, Z) for measurement resulted in one-third random selection.

While the QKD protocol has perfect unconditional security in theory, it fails miserably when put into practice and is vulnerable to quantum attacks. One photon is sent to Bob, and the other is taken by the attacker to look for the key in a standard communication system. This is called a photon splitting attack, which is also called a storage attack. Decoy state [38] strategy was meant to keep the enemy from being able to tell the difference between single and multiphoton keys. Another procedure to stop the PNS attack by SARG. [39] used the same method as BB84, but instead of comparing the basis, it looked at one of four non-orthogonal states. This made the chance of detection drop from 50% to 25%. Several other protocols have utilized the same strategy in quantum communication but utilized a different procedure in classical to prevent the decrease of raw keys and produce finite keys from communication [40].

B. Ekret B91

Among the many quantum mechanical properties relevant to safe communication is entanglement. If two quantum bits are maximally entangled and widely apart, then measuring one bit will have a direct correlation with measuring the other bit. his makes it a safe security system.

Working model of the Ekret protocol.

- An 'n' EPR pair with a maximum entangled state is generated by external sources, and an individual pair of qubits is then sent to Alice and Bob.
- To get results with -1 and +1 at both ends,
- Alice (a1=0.a2=º ‸a3=…º ..)
- Bob (b1=0.b2=º ‸b3=†º ‸..)
- calculated their measuring angles. After quantum transmission,
- Alice and Bob tell everyone about the direction and split into two groups. 1.
- The same direction was used or the key generation 2.
- Adversaries can be found by their different orientations.

In the initial group, the likelihood of each participant having an identical orientation is 2/9, or (a1, b1) and (a2, b2). To identify Eve's presence in Communication, the remaining unsuccessful probability is utilised to establish a correlation coefficient in the second group.

E(ai,bj) = P00(ai,bj) -P01(ai,bj) -P10(ai,bj) + P11(ai,bj) (5) where P00 stands for both Bob and Alice getting the "0" bit and P01, P10, and P11 do the same for Alice and Bob. The equation (5) value is utilised in CHSH to check Eve's violation.

S = E(a1,b2) + E(a1,b3) - E(a3,b1) + E(a3,b3)

If S is between -2 and 2, it means that the qubits are not fully entangled, disturbed, or there is an adversary in the

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

communication. If S is between -2 and 2, it means that the communication is safe. The fundamental will be made with the same orientation analyzer and used for encryption once the connection is no longer being interrupted.

The practical implementation of an Entanglement-based protocol faces the challenge of photon splitting attacks; several protocols have devised solutions to overcome it.

Initially, weak coherent pulses are employed to generate photons with decoy states with probability 'f' and without decoy states with probability '(1-f)/2', as well as a timestamp. The encoded classical bit associated with decoy states is removed in classical communication to obtain raw keys. Produce a feeble coherent pulse that is phase converted and has a time delay between two consecutive pulses to observe the variation of the receiver detector.

Recently, there have been many improvements made to the field of quantum key sharing by taking into account the problems that still come up when they are used in context. In all communication systems, communicating channels are regarded as risk and susceptible to information leakage.

However, what if a communicating device is in danger? So, Device Separated Quantum Key Distribution (DIQKD) has been placed into place, where trustworthy parties will randomly measure to verify the source's trustworthiness and construct a key, or use Heisenberg or Entanglement principles to generate a photon. Attackers could target the measuring side channels. In this case, Measurement device independent Quantum key distribution (MIQKD) would let a third party do the measuring. Right now, it's not practical for everyone to use a quantum device at the same time. To work around this, a SQKD (semi classical Quantum key Distribution) is used, where one user fully uses quantum capabilities and another user partially does so. Ping-pong methods were used to make the QKD key for QSDC protocols.

V. QUANTUM INTEGRATION WITH IOT FRAMEWORK\

The present era application operates continuously for an entire year, necessitating an automated process to manage and monitor the work. Due to the difficulty of this task, an IoT-based automated process was utilised. While the early stages of the Internet of Things (IoT) make things easier to use, the fact that unauthorised people can access them has caused a lot of worry in modern times. Let's look at some real-world examples of IoT applications and how security affects their use.

Many billions of devices are linked together and talking to each other without any help from people. This is called the internet. More IoT devices mean more threats and security problems in connectivity. Because of this, many security factors should be carefully considered before creating an IoT system in the conventional method.

1. Users should make strong passwords and change them often.
2. IoT software in IoT devices should be updated often to stop new threats.

3. IoT devices, gateway, Edge router, Edge server, and cloud can talk to each other safely.

Because of Shor's Algorithm, the growth of quantum technology has made hackers more adept at using it than the classical model. Shor developed a method for calculating the prime factor of a big integer in polynomial time, as opposed to the traditional model, which requires exponential time. Right now, all security depends on the RSA model, which is hard to understand because it involves factoring a big number.

All Internet of Things (IoT) devices talk to the Edge node (mobile phones) through the Gateway. The Edge node tells the devices how to work. The Edge node will send critical data to the cloud for storage via the Edge server and conduct additional analysis of IoT device operation and reliability. A hacker can access all IoT levels from devices to the cloud network, and any leak or assault at any layer gives them information.

Consider the following Internet of Things scenario: a parent wishes to provide care for their child in real time, regardless of whether the youngster is in the home or at the workplace network. The Edge device in the home network is connected to the IoT devices through routers, as each device has a unique IP address. EdgeNode in home network is thought to be safer than outside network, since parents can directly watch and control IoT device whenever there is a threat. Edge nodes can transmit threat and attack data to the cloud network, which can then be used to detect future occurrences of the same type of threat.

In an outside home network, IoT devices' messages must travel far to reach the EdgeNode. Security vulnerabilities will rise since data would transit across gateway and many edge

***Article Received:** 25 November 2023 **Revised:** 12 December 2023 **Accepted:** 30 January 2024*

servers, giving hackers plenty of opportunities. The parent verifies the data obtained from different IoT devices using the EdgeNode Application interface and takes action according to the current state.

VI. CONLCUSION

A smart home, health care, and business processes can all be monitored and developed with the help of the Internet of Things (IoT). This is what today society wants is. The rapid growth of Internet of Things devices does not provide the speed boost that is provided by the conventional computer model, and it also raises the risk of hackers gaining access to private information. Quantum computing, the growth of long-lasting, cutting-edge technology, is both good and bad for the traditional world. Quantum computing is advantageous because it expedites computation and reduces the complexity of resolving complex problems that require exponential time to resolve in the classical domain. Quantum computing uses reversible computing to get the input from the output so that heat energy isn't lost like in normal physics. Quantum Oracle and Quantum Fourier transform show the qubit in a superposition state to allow parallelism, which speeds up the process. This is a bad thing because hackers can use speedup computation to break the encryption method in a very short amount of time and get private information. Quantum hacking can be avoided by adopting quantum encryption, as quantum behaviour is deterministic and leads to the identification of adversaries during communication. Ping-pong and LM05 are two-way communication protocols (QSDC) that allow secure contact without creating a key, but they can be broken by a quantum attack Quantum hacking can be stopped by using the QKD protocol, which uses the Heisenberg and Entanglement principles of quantum physics as an OTP in the classical model. This is a safe way to communicate for a single point of use. The IoT security issues can be resolved by integrating quantum properties into the IoT framework to ensure the secure transmission of information from end-to-end node communication.

References:

[1] Atzori ., Iera A., and Morabito G., ‘The Internet of Things: A survey ’. *Computer Networks*. 2010; 54(15): 2787–2805

[2] Mouzhi Ge,Hind Bangui,Barbora Buhnova., Big Data for Internet of Things: A Survey, Future Generation Computer Systems 2018, 4:053

[3] Sachin Kumar, Prayag Tiwari, Mikhail Zymbler ,. ‘Internet of Things is a revolutionary approach for future technology enhancement: a review’. *Journal of Big Data*:2019;6(1)

[4] Timothy Malche, Priti Maheshwary, ‘Internet of Things (IoT) for building smart home system’. *International Conference on I-SMAC;* Palladam, India, Feb. 2017. IEEE: Oct 2017

[5] Gordon E. Moore, 'Cramming more components onto integrated circuits' *Electronics*:1965; 38(8):114-117

[6] Theis H., Philip Wo S.,'The End of Moore's Law: A New Beginning for Information Technology'. *Computing in Science and Engineering*:2017; 19(2):41-50

[7] Christopher Havenstein,Damarcus Thomas,Swami Chandrasekaran,. ‘Comparisons of Performance between Quantum and Classical Machine Learning’. *SMU Data Science Review*:2018; 1(4):11

[8] Shor P W., ‘Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer’. *SIAM Journal of Computing*. 1997; 26(5):1484–1509

[9] http://cryptomuseum.com/crypto/otp/index.html

[10] Marius Krumm, Markus P. Mueller.,'Quantum computation is the unique reversible circuit model for which bits are balls'. *npj Quantum Information*. 2019;5(7)

[11] Nielsen M.A., Chuang I.L., *Quantum computation and quantum information.* Cambridge University Press;2012.p.

[12] David Deutsch., ‘Quantum computational networks’. *Proceedings of the Royal Society of London Series A*, London, Sep 1989; 425(1868):73–90

[13] Lov K. Grover., ‘Quantum computers can search arbitrarily large databases by a single query’. *Physical Review Letters*. 1997; 79(23):4709–4712

[14] Lov K. Grover., ‘A framework for fast quantum mechanical algorithms’. *In Proceedings of STOC.1998*;p 53–62,

[15] Donald C Chang., ‘Physical interpretation of the Planck’s constant based on the Maxwell theory’. *Chinese Physics B*. 2017; 26(4)

[16] John S. Bell., ‘On the Einstein-Podolsky-Rosen paradox’. *Physics.1964;* 1:195–200

[17] Dirk Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, HaraldWeinfurter, Anton Zeilinger., ‘Experimental quantum teleportation’. *Nature. 1997*, 390:575

Article Received: *25 November 2023* ***Revised:*** *12 December 2023* ***Accepted:*** *30 January 2024*

[18] Charles H. Bennett,Stephen J. Wiesner., ‘Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states’. *Physical Review Letters. 1992*; 69:2881–2884

[19] Wootters W.K., Zurek W. H., “A single quantum cannot be clone’, *Nature*. 1982; 299(5886):802-803

[20] Bostr¨om, K., Felbinger, ‘Deterministic secure direct communication using entanglement’. *Physical Review Letter*.2002; **89**(18):187902

[21] Qing-Yu, C., Bai-Wen, L., ‘Deterministic secure communication without using Entanglement’. *China Physic Letters*.2004; **21**(4), 601

[22] Cai, Q.Y., Li, B.W., ‘Improving the capacity of the bostr¨om-felbinger protocol’. *Physical Review A*.2004; **69**(5), 054301 (2004)

[23] Gao, T., Yan, F.L., Wang, Z.X., ‘Deterministic secure direct communication using GHZ states and swapping quantum entanglement’. *Journal of Physics A: Mathematical and General*.2005; **38**(25),5761

[24] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu1, Gui Lu Long., ‘Quantum secure direct communication with high-dimension quantum superdense coding’. *Physical Review A. 2005;***71**(4), 044305

[25] Jian Li, Zeshi Pan, Fengqi Sun, Yanhua Chen., ‘Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state’. *Entropy*.2015; 17(10):6743–6752

[26] Deng, F.G., Long, G.L., ‘Secure direct communication with a quantum one-time Pad’. *Physical Review A*.2004; **69**(5), 052319

[27] Dong Jiang, Yuanyuan Chen, Xuemei Gu, Ling Xie & Lijun Chen., ‘Deterministic secure quantum Communication using a single d-level system’. *Scientific Reports*.2017; **7**:44934

[28] Guerra, A.G.A.H., Rios, F.F.S., Ramos, R.V., ‘Quantum secure direct communication of digital and analog signals using continuum coherent states’. *Quantum Information Process.2016;* **15**(11): 4747–4758

[29] Nguyen B A., ‘Quantum dialogue’. *Physics Letters A*. 2004;328(1):6–10

[30] Wang, H., Zhang, Y.Q., Liu, X.F., Hu, Y.P., ‘Efficient quantum dialogue using entangled states and entanglement swapping without information leakage’. *Quantum Information Process.2016;* **15**(6):2593–2603

[31] Bennett C. H., Brassard G., ‘Quantum cryptography: Public key distribution and coin tossing’, *Theoretical Computer Science*. 2014, 560(1):7-11

[32] Ekert A. K., ‘Quantum cryptography based on Bell’s theorem’, *Physical Review Letter*. 1991; 67(6):661.

[33] Mario Stipcevic, Cetin Kaya Koc., ‘True random number generators’, *Open Problems in Mathematics and Computational Science*. 2014; p. 275-315

[34] Agoston Schranz and Eszter Udvary, ‘Quantum Bit Error Rate Analysis of the Polarization based BB84Protocol in the Presence of Channel Errors’. *Proceedings of the 7th International Conference on Photonics, Optics and Laser Technology*. 2019; 1:181-189.

[35] C. H. Bennett, ‘Quantum Cryptography using any two Non orthogonal States’. *Physical review letters*.1992; 68: 3121-3124

[36] H. B. Pasquinucci and N. Gisin, ‘Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography’. *Physical Review Letter A*.1999;*59:* 4238-4248

[37] Dagmar Bru, ‘Optimal Eavesdropping in Quantum Cryptography with Six States’, *Physical Review Letter.* 1998; 81(14):3018-3021

[38] Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, ‘Decoy State Quantum Key Distribution’ *Physical Review Letters*.2005;94:230504

[39] V. Scarani, A. Acin, G.Ribordy, and N. Gisin, ‘Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations’. *Physical Review Letters.* 2004*;* 92(5).

[40] M. M. Khan, M. Murphy, A. Beige, ‘High error-rate quantum key distribution for long distance communication’, *New Journal of Physics.* 2009,11(6):63043