ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security

Niravkumar Prajapati[1]

[1]Independent Researcher

Publication Date: 2025/05/28

Abstract: Quantum computing is poised to revolutionize numerous sectors, with cryptographic security identified as one of the most critically affected domains. For instance, Elliptic Curve Cryptography (ECC) and RSA, two traditional encryption techniques, rely on the computational difficulty of integer factorization and discrete logarithms. Nevertheless, quantum algorithms, particularly Shor's algorithm, which jeopardizes the security of existing cryptographic systems, may be able to address these problems successfully. This discovery necessitates the development of cryptographic techniques that are impervious to quantum attacks. The study of post-quantum cryptography (PQC), which includes hash-based, lattice-based, and other quantum-resistant algorithms, is becoming essential to ensuring the long-term confidentiality and integrity of data. This paper explores the basic concepts of quantum computing, their relationship to cryptographic privacy, and potential solutions for the associated security problems in the quantum age.

Keywords: *Quantum Computing, Cryptographic Security, Shor's Algorithm, RSA, ECC, Post-Quantum Cryptography, Lattice-Based Cryptography, Hash-Based Cryptography, Quantum-Resistant Encryption, Cybersecurity, and Quantum Threats.*

How to Cite: Niravkumar Prajapati (2025). Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security. *International Journal of Innovative Science and Research Technology,* 10(5), 2023-2035. https://doi.org/10.38124/ijisrt/25may501

I. INTRODUCTION

Quantum computing, inspired by a paradigm change in computing power, is represented by the concepts of quantum mechanics, which allow for computations to be performed at exponentially faster rates than those of conventional computers. The fundamentally different quantum bits, or qubits, Classical bits are the foundation of this innovative technology [1]. The superposition principle allows for the simultaneous existence of many states, as opposed to traditional bits, which are simply qubits, which can be either 0 or 1. Their unique ability to process data in parallel makes quantum computers perfect for solving difficult problems in domains like cryptography, optimization, and simulation.

The concept of superposition, along with strong quantum algorithms are built on the foundation of entanglement and quantum interference. Notably, Grover's algorithm enables significantly faster unstructured search, and Shor's algorithm makes it possible to factor big numbers quickly, which puts traditional encryption techniques like RSA and ECC in serious danger [2]. These capabilities signal a looming challenge to current cryptographic infrastructures, which mostly depend on the computational complexity of certain security-related issues.

As quantum computing technology progresses toward practical implementation, it raises critical cybersecurity concerns, particularly for nations like the United States [3][4]. The potential for quantum systems to crack traditional encryption in realistic timeframes highlights the urgent need to develop post-quantum cryptography, or PQC. PQC aims to develop cryptographic algorithms that are impervious to quantum attacks in order to protect data in a future where quantum dangers are prevalent.

Transitioning to PQC does not simply require replacing existing algorithms but a fundamental reassessment of encryption systems and practices. Promising choices for quantum-resilient algorithms include code-based encryption, lattice-based cryptography, hash-based methods, and multivariate polynomial cryptography.

The influence of quantum computing goes beyond cryptography to fields like materials research and medical development, demonstrating its enormous potential. However, a proactive strategy in the area of digital security is required due to the technology's dual-use nature [5]. As communication systems and digital infrastructure evolve, integrating quantum-resilient cybersecurity measures becomes a strategic imperative. Preparing for the quantum era involves anticipating both its transformative power and its inherent risks, emphasizing the necessity of safeguarding digital assets before quantum computing becomes widespread.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

II. OVERVIEW OF QUANTUM COMPUTING

The field is undergoing a paradigm shift thanks to quantum computing, which offers previously unheard-of processing capability that may be able to resolve issues that traditional computers are unable to handle. This transformative technology, however, does not come without its implications for cybersecurity [6][7]. As it approach this new frontier, it is critical to understand the opportunities and challenges it brings, particularly in the context of safeguarding the United States' digital assets [8][9]. Quantum computing operates on the fundamentals of quantum physics, which uses superposition and entanglement to do calculations at speeds that are not achievable with traditional computing methods. This capability is not merely an incremental improvement but a noteworthy development that might revolutionize fields like medication development and cryptography [10][11]. The advent of quantum computing marks the start of a new technological age, where integrating it into cybersecurity frameworks is both essential and difficult. Figure 1 shows the Quantum Computing 101 brief overviews.

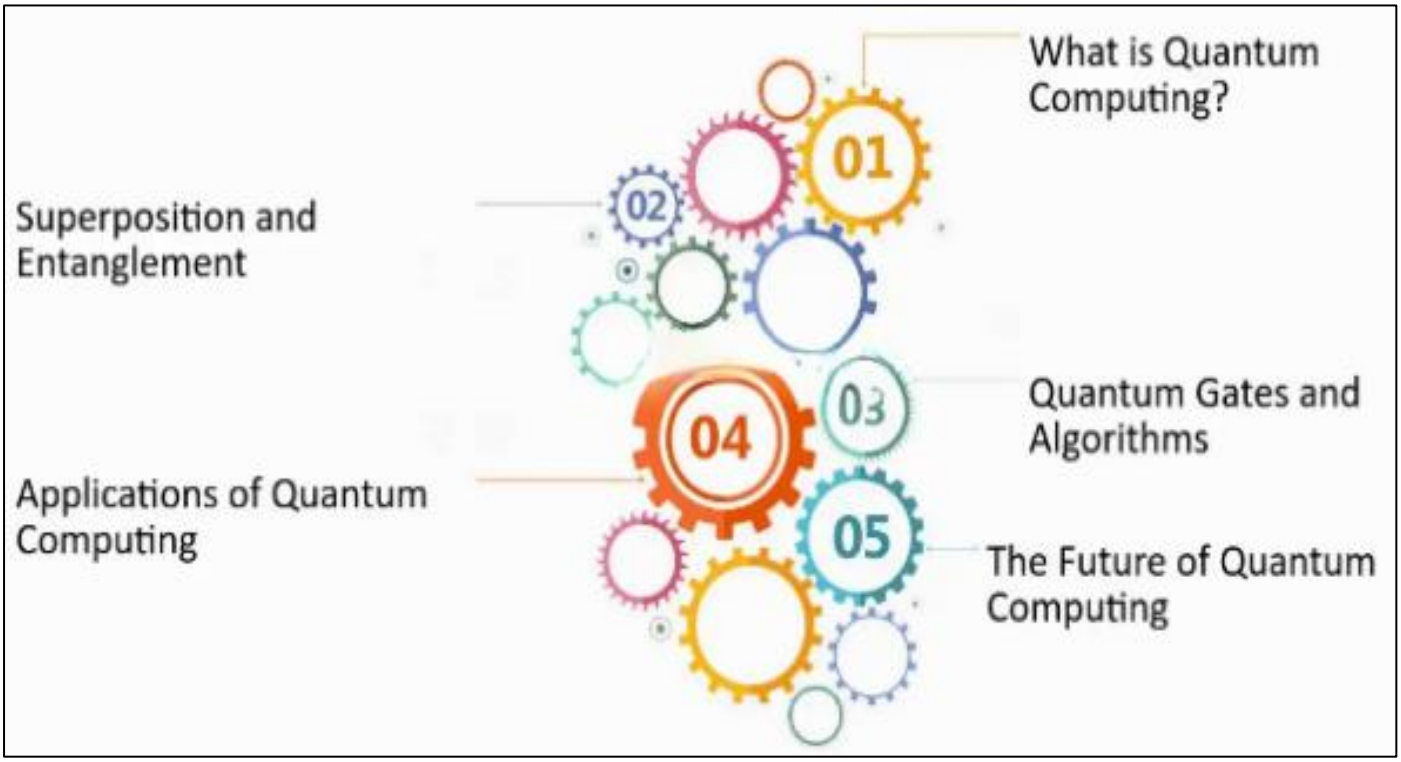

Fig 1 Quantum Computing 101 a Brief Overview

In order to manage the intricacies of the interaction between protection and quantum computing, which is a dynamic and dynamic sector, constant study, cooperation, and policy development are needed [12][13]. Because digital security might be strengthened or undermined in light of quantum computing, a proactive and knowledgeable approach to cybersecurity is required in the quantum era. In order to ensure a safe and robust digital future for the United States, it is crucial to strike a balance between the need to safeguard against possible threats and the pursuit of quantum computing's benefits as continue to investigate how these technologies affect digital security [14].

- *Importance of Cryptographic Security*

Data encryption is the process of encoding or concealing information so that only the intended recipient can decode it. It is still utilized today in passwords, debit and credit card machines, and e-commerce, where it has been employed for thousands of years to encrypt communications.

Encoding data such that only the intended recipient can read and process it is known as cryptography. It is commonly referred to as cryptography [15][16]. Combining a variety of disciplines, such as engineering and computer science, and mathematical information, this counterterrorism technique, also known as cryptology, generates complex encryption that hides the true content of the communication.

Cryptography, which has its origins in ancient Egyptian hieroglyphics, is crucial for the security of data and information at rest and in motion and for preventing unauthorized access. It uses methods like digital signatures and cryptographic keys, mathematics, and mathematical concepts to encrypt communications, making them difficult to understand. This protects financial transactions, emails, web browsing, and personal data [17][18].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

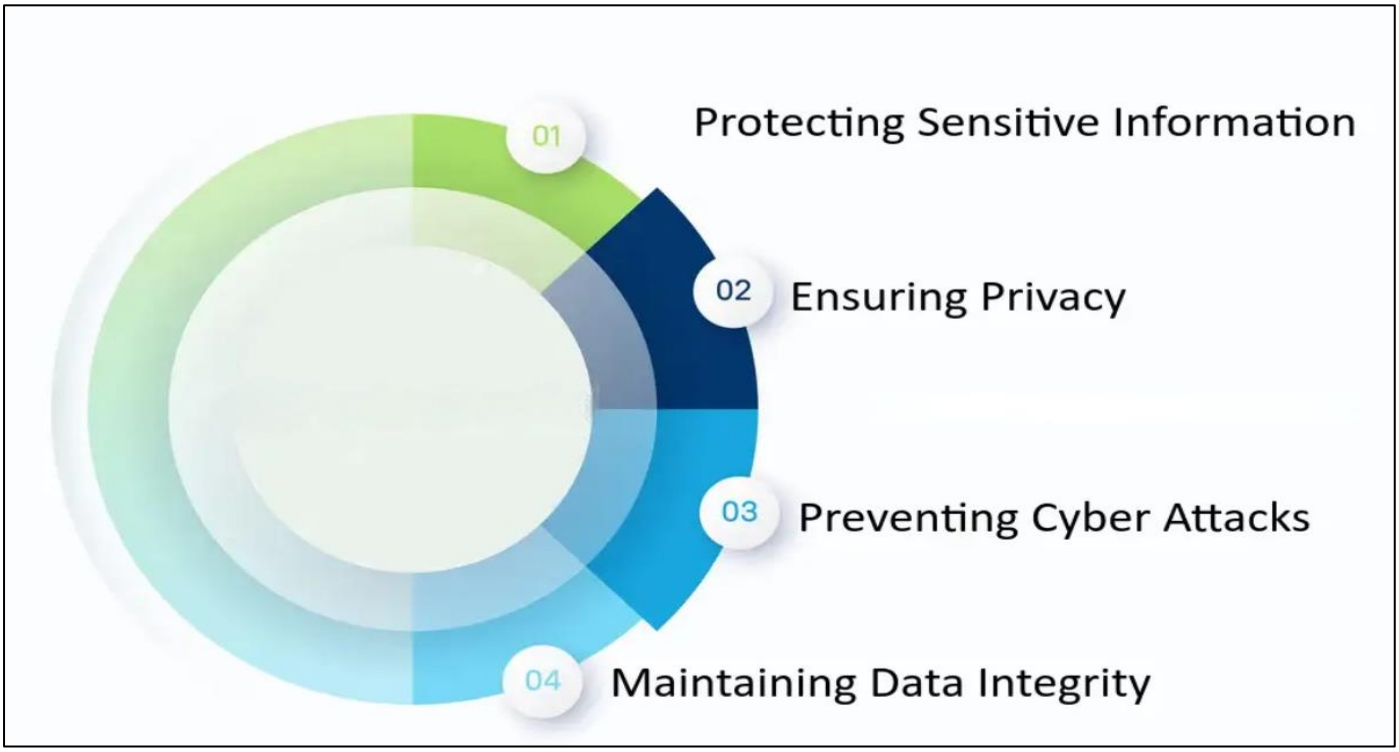

Fig 2 Importance of Cryptography

➢ *The Importance of Cryptography*

The art of Secrecy, consumer and data protection, and the prevention of fraud involving private corporate data all rely on encryption. The following are examples of typical cryptographic uses and examples shown in Figure 2:

- *Privacy and Confidentiality*

People and businesses rely on cybersecurity measures on a daily basis to protect sensitive information, keep online discussions private, and prevent unauthorized access to sensitive data [19]. Cryptography protects sensitive information by encrypting messages using a public key that only the sender and the receiver are aware of [20]. The famous messaging software, WhatsApp, is a good example of this since it encrypts user messages to make them unbreakable [21].

Another way that cryptographic protects surfing is via VPNs, which include asymmetric encryption, which uses publicly and privately shareable keys and protected passageways.

- *Integrity*

Cryptography is a powerful tool for ensuring the authenticity of messages and the security of data in transit. Encryption prevents content tampering both at rest and in transit between the sender and the recipient [22]. In financial transactions and software delivery, for example, digital signatures can detect tampering or forgeries.

- *Nonrepudiation*

The sender of a communication cannot subsequently retract what they meant while creating or transmitting information since cryptographic verifies their transparency and accountability. An excellent illustration of this is the use of digital signatures that ensure the sender cannot assert forgery of a message, contract, or document. When it comes to email confirmation, email tracking also makes sure that no one can claim they didn't send or receive an email.

➢ *Principles of Quantum Mechanics (Superposition, Entanglement, Quantum Processing Unit)*

Numerous scientific jobs may be completed by machines, which are widely used and very powerful, in economy, daily living, and education. Anyone with the means to purchase a mobile phone or laptop can access them [23]. Regardless of the incredible advancements in power processing that have been driven by microelectronics [24][25].

The four main components of a standard digital computer system are the main memory, ALUs, control units, and input/output ports. Researchers are increasingly focused on developing quantum computers due to the fact that regular computer frameworks**,** even with the help of modern supercomputers, are unable to tackle the most challenging jobs. In tandem with AI, the context of the coming years, one of the most significant scientific and technological problems will be quantum computing shown in Figure 3 [26].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

Fig 3 Quantum Mechanics

- *Superposition*

The well-known double-slit experiments illustrate how, in the realm of quantum physics, entities like photons do not always have distinct states. The single particle of light travelling through a screen with two tiny holes in this arrangement would cause an interference structure on a photographic screen that resembles the pattern created by light waves; this may be seen as an accumulation of all possible routes. The interference pattern disappears when the photon's crossing of one of the slits is determined using an instrument [27][28]. This unexpected result is understood to mean that every potential configuration of a quantum system "exists" beforehand the system collapses into a single state due to a measurement that introduces a deadly disturbance; this phenomenon is known as decoherence. The reproducibility of this phenomenon in computing held the promise of a steady rise in processing power [29].

A conventional digital computer uses binary a 4-bit computing registration, for instance, may store any one of 16 bits, which are figures that may reside stored in either of two indicates, denoted by the numbers 0 and 1 (2^4) possible numbers. In contrast, a qubit, for instance, a 4-qubit computer's registration can accommodate 16 distinct integers because at the same time, it occupies a wavelike space between the integers 0 and 1.

- *Entanglement*

The entanglement is the qualitative equivalent of juxtaposition, which is the capacity of a qubit to exist in more than one state at once, such as 0, 1, or any mixture of both phenomena when a correlation develops between two or more quartz quantum bits. That is, one qubit's situation cannot be defined without reference to the state of its partner or colleagues. Entangled qubits may quickly communicate knowledge with each other, regardless of how far apart they are, thanks to this reliance. This occurrence, which Einstein disliked because of quantum physics's non-local and unpredictable nature, he called "spooky action at a distance." Many quantum computing techniques rely on interaction to solve challenges more quickly and effectively.

- *Quantum Processing Unit*

The fundamental part of technology for quantum computing, a QPU, processes qubits via a series of quantum gates for quantum algorithm implementation. QPUs manage qubits, allowing quantum computers to do complicated tasks tenfold faster than their classical counterparts. Normal processors, who process such as CPUs, GPUs, and DPUs (data handling units widely used in data centers), make use of the laws of classical music and the laws of physics to perform tasks. Photonic chips, superconducting qubits, nuclear magnetic resonance, and trapped ions are some of the underlying technologies, may be used in QPUs; each has benefits and disadvantages of its own.

Quantum computing is becoming increasingly recognised as one of the most revolutionary technologies available, but it has strict limitations. A quantum computer has to sustain quantum entanglement, or coherence between its qubits, over an extended period of time in order to run a whole algorithm [30][31].

➢ *Quantum bits (Qubits) vs. Classical Bits*

The nature of quantum computers often requires more regulated physical conditions to operate than traditional computers due to quantum physics. The processing power and scalability of conventional computers are lower than that of quantum computers. Furthermore, their data units differ: conventional computers use bits, whereas quantum computers utilize qubits.

- *Units of Data: Bits and Bytes vs. Qubits*

In conventional computers, data is processed in a binary manner.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

The fundamental data unit used by classical computers is bits; eight units of bits are called a byte. Code on classical computers is written as a binary number, either 1 or 0. In short, these 1s and 0s stand for the states of on and off, respectively. For instance, they may show true or false or yes or no [32].

This procedure, which is sequential in nature and necessitates finishing one job before proceeding to the next, is sometimes called processing in series. In order to do several calculations at once, many computer systems use heterogeneous manufacturing, which is an extension of classical processing. Additionally, classical computers only provide a single output since binary bits of 1s and 0s might be repeated [33].

In contrast, quantum computing has its own set of rules. A qubit is the information unit used in quantum computers. In contrast to bits, which can only be either 1 or 0, qubits may be in several states at once and be both 1 and 0. The juxtaposition is the term for this situation, in which characteristics are unfamiliar until they are assessed [34].

The algorithms used on traditional computers require a large number of simultaneous calculations to solve issues. When analyzing data under a wide range of limitations, quantum computers may consider many possible conclusions [37]. There is a likelihood connected with the conclusions, and quantum computers are capable of doing more complex computations than traditional computers. This is shown in Figure 4.

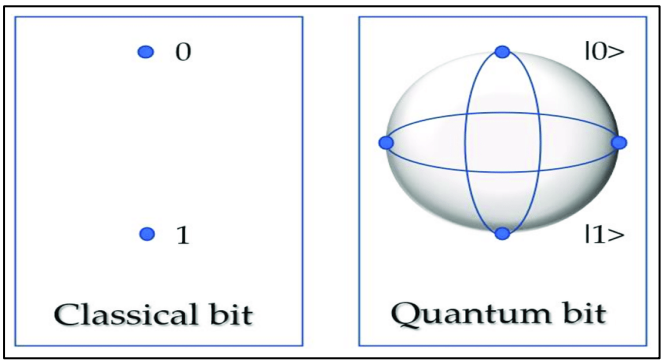

Fig 4 Classical vs Quantum bit

- *Power of Classical vs. Quantum Computers*

The majority of Boolean logic and algebra are used in classical computers, and power increases linearly with the amount of 1s and 0s in the system due to the transistor count. The direct connection indicates that in a traditional computer [35].

III. CLASSICAL CRYPTOGRAPHY AND ITS SECURITY

Knowledge concealment is accomplished by the use of classical the use of cryptography, which encrypts plain text messages by converting them into incomprehensible ones [36][37]. In addition to encrypting plain text, Quantum cryptography offers total data transmission security using the principles of quantum physics. It uses quantum knowledge to detect intrusions, especially eavesdropping, and it employs a cryptographic system based on the idea of quantum mechanics [38]. The ideas of safely communicating process systems, however, are best illustrated by classical quantum cryptography, which employs the safe circulation of keys. These concepts are also used in quantum key exchange. In this research, they examine the literature on quantum and conventional cryptography and compare them based on data categorization, security level, and time. The advantages of classical and quantum cryptography in many different situations are also highlighted, along with a brief study of perspective classical cryptography and the idea of quantum cryptography with alternative protocols [39]. Lastly, they provide a list of suggestions for choosing the best decryption type to protect the connection.

The colleagues know, their survey is the first in-depth discussion of quantum-based approaches to 5 G-enabled IoT security, quantum-resistant techniques, and 5 G-enabled IoT security and privacy issues [40]. As a manual to help future researchers comprehend and use the current techniques, it also looks at the corpus of work offered up to 2023. The purpose of the essay is to offer new perspectives that haven't been thoroughly examined in previous publications, including:

- It is crucial to look at the technological underpinnings of 5G with regard to IoT needs, perspective, and current developments in 5 G-enabled IoT, given the ongoing advancements of IoT connectivity systems enabled by 5G and their extensive use.
- An in-depth examination of the needs and goals to exploit 5G's advantages for upcoming IoT applications.
- A thorough analysis of the security issues and weaknesses in 5 G-capable Internet of Things devices by classifying them into five main applications: IoT in linked homes, smart agriculture, e-healthcare, and industries [34].
- An overview of significant advancements and studies in authentication systems and key management protocols for Internet of Things connectivity, as well as the security problems and difficulties that must be resolved in a post-quantum world.
- A thorough examination of the attackers' capabilities through in-depth conversations**.**
- The survey provides post-quantum-resistant authentication techniques in detail for 5G-enabled After discussing how standard cryptography primitives have been impacted by quantum computing, the primary objective is IoT [41].
- List and talk about the synchronization and uncertainty principles-based QKD approaches, as well as the methods that will be taken into account to guarantee simultaneous authentication.
- A thorough analysis of the key issues, potential research areas, and comparison of conventional and quantum-resistant methods for authentication in order to create a secure IoT framework allowed by 5G [42].

➢ *Classical Cryptographic Methods*

It includes spreadsheets, the criteria for the requirements, exclusion, search criteria, and the application review procedure [42]. Figure 5 shows the Cryptographic process. Two-tiered assessment and security considerations comprise the selection procedure for documents:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

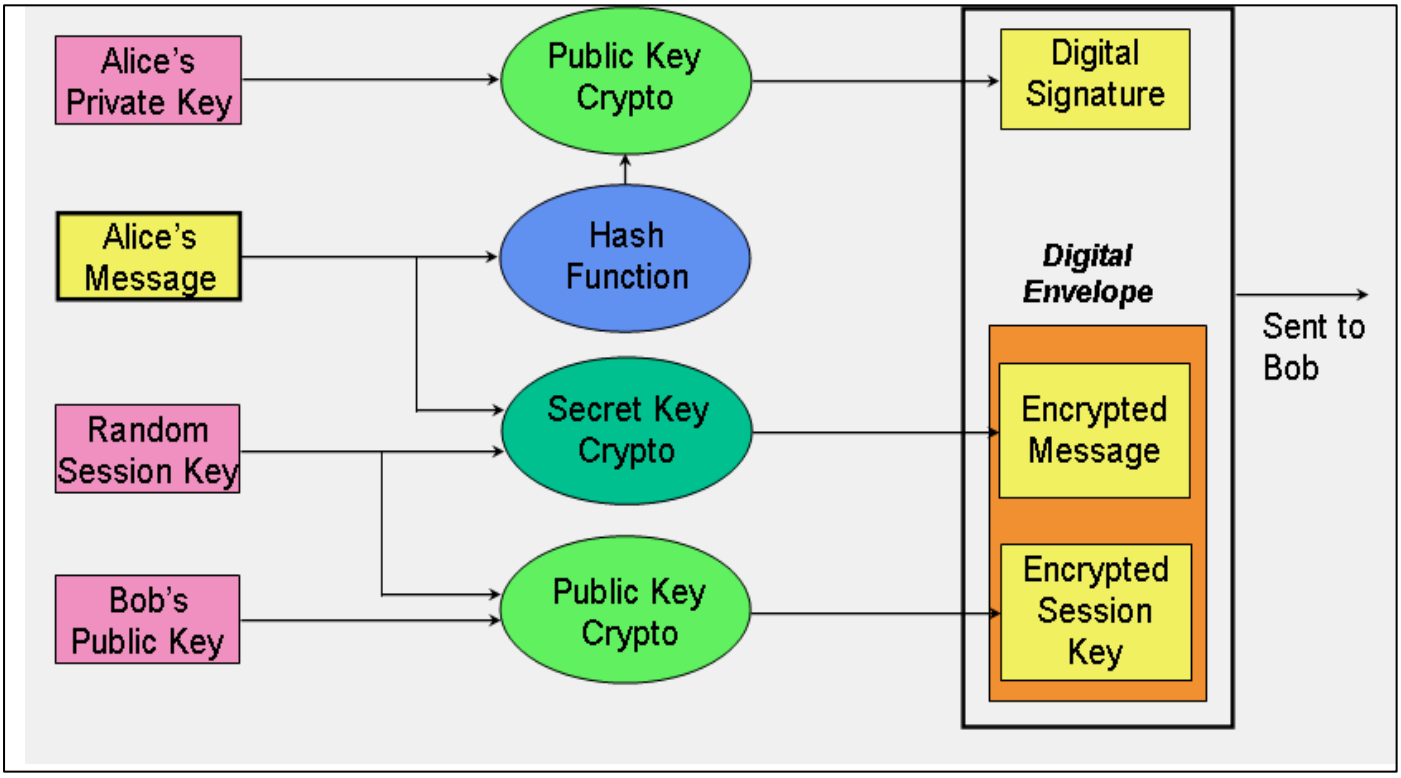

Fig 5 Cryptographic

- **Title and Abstract level Screening:** First, two important articles based on PQC and QC from 2021 and 2022 were included in the selection of papers from 1989 to 2023 that were taken into account. At this stage of screening, it applied inclusion/exclusion criteria to both the title and the abstract of the article. Both writers conducted their own independent analyses of the search results and used dialogue to settle any disputes.
- **Full-Text Screening:** At this stage, it applied both inclusion and exclusion requirements after thoroughly analyzing the manuscript. Nonetheless, if it came across two studies that examined related material, it took into account the one that offered more thorough information.
- **Security Criteria:** Conducted a security study with the goal of extracting articles that had enough knowledge on existing IoT security solutions, such as key management, authenticating each other, and algorithmic cryptography, as well as security challenges enabled by 5G. A few chosen IoT security studies have focused on the use of quantum solutions (quantum cryptography or post-quantum cryptography) in various IoT scenarios, including smart medical therapy, smart homes, and smart neighborhoods. A thorough examination of the chosen security flaws and existing solutions in order to develop new avenues based on:
- **Quantum-security context:** The chosen papers must include enough details on how security concerns in the wide field of IoT are being addressed by utilising quantum-resistant technologies.
- **Quantum authentication:** The quantum authentication-based studies take advantage of key management problems and provide fixes.

Investigations into IoT security vulnerabilities are conducted using the quantum-enabled security technologies mentioned above. It is essential to comprehend the limitations of conventional encryption and the possibilities of quantum technology for safe communication between Internet of Things devices since the research raised enough IoT security concerns [43].

IV. KEY CRYPTOGRAPHIC ALGORITHMS

The review of post-quantum cryptography methods being created to withstand quantum assaults and an outline of the traditional cryptographic algorithms most affected by quantum computing [44]. There are some algorithms are discussed below:

A. Rivest-Shamir-Adleman (RSA)

The acronym for RSA, those who discovered RSA, sometimes established as the public key procedure, is the most popular and well-known asymmetric algorithm. To make it quicker and more secure, it has combined RSA and ECC in their suggested work. Since RSA utilizes the decryption key and the decryption key in a single pair, it is highly helpful for sharing secret or confidential information between two parties without the need for an intermediary [45].

The stages of the RSA algorithm are as follows are shown in Figure 6:

➢ *Generation of Pair of Keys*

The public key serves as the basis for the usage of encryption, and the private key is used to decode. In RSA, two keys are generated: the public key and the private key. The following are the steps to generate keys:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

- Select two unique prime numbers, a and b.
- Then it compute x = a×b
- Then it compute α= (a − 1)(b − 1)
- The next step is to choose an integer c that satisfies the prerequisites.

1 < c < α

c and α should be co-prime

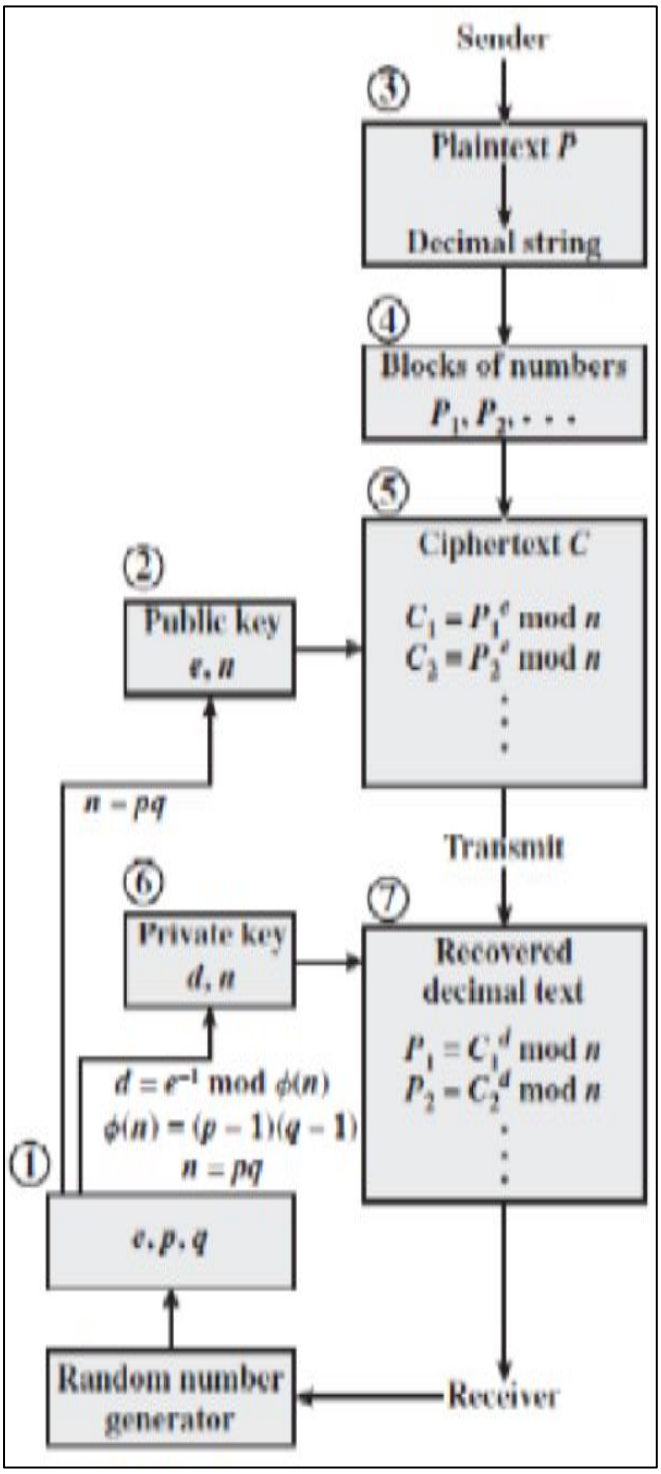

Fig 6 Working of RSA

The exponent of the public key, which is c, is revealed, meaning that the public key is comprised of c and α.

➢ *Generating Private Key*

In this case, it find d's value by executing c (mod α), which is the same as saying that cd=1 (mod α). The secret password exponent is the numerical value of d, which means that the private key is made up of d and α**.**

➢ *Encrypting with Public Key*

Following these procedures describe how RSA encrypts data using the public key exponent:

- The plaintext is transformed to P, where P is the initial value that belongs to {0, 1…., (a×b)-1}
- Then it compute M = pc mod n where n=a×b.
- The decryption with a secret password the private key multiplier in RSA is used to decode data.
- The necessary procedures are:

Compute Md = p (mod n)

B. Data Encryption Standard (DES)

According to advised to use the same key for both encryption and decryption when using the symmetric data encryption standard [46]. Before it broke and went out of style, it was frequently utilized. The dimension of the block was tiny, and the key size was modest.

C. DES Algorithm Consists of the Following Steps

DES accepts each containing 64 bits of plaintext and a key, eight of the 64-bit key's bits are known as parity bits shoen in Figure 7, which are used to determine if the key being used is comparable to the one that was ultimately chosen. The key now has 56 bits instead of 68 after removing these 8 bits. The algorithm will subsequently make use of this [47].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

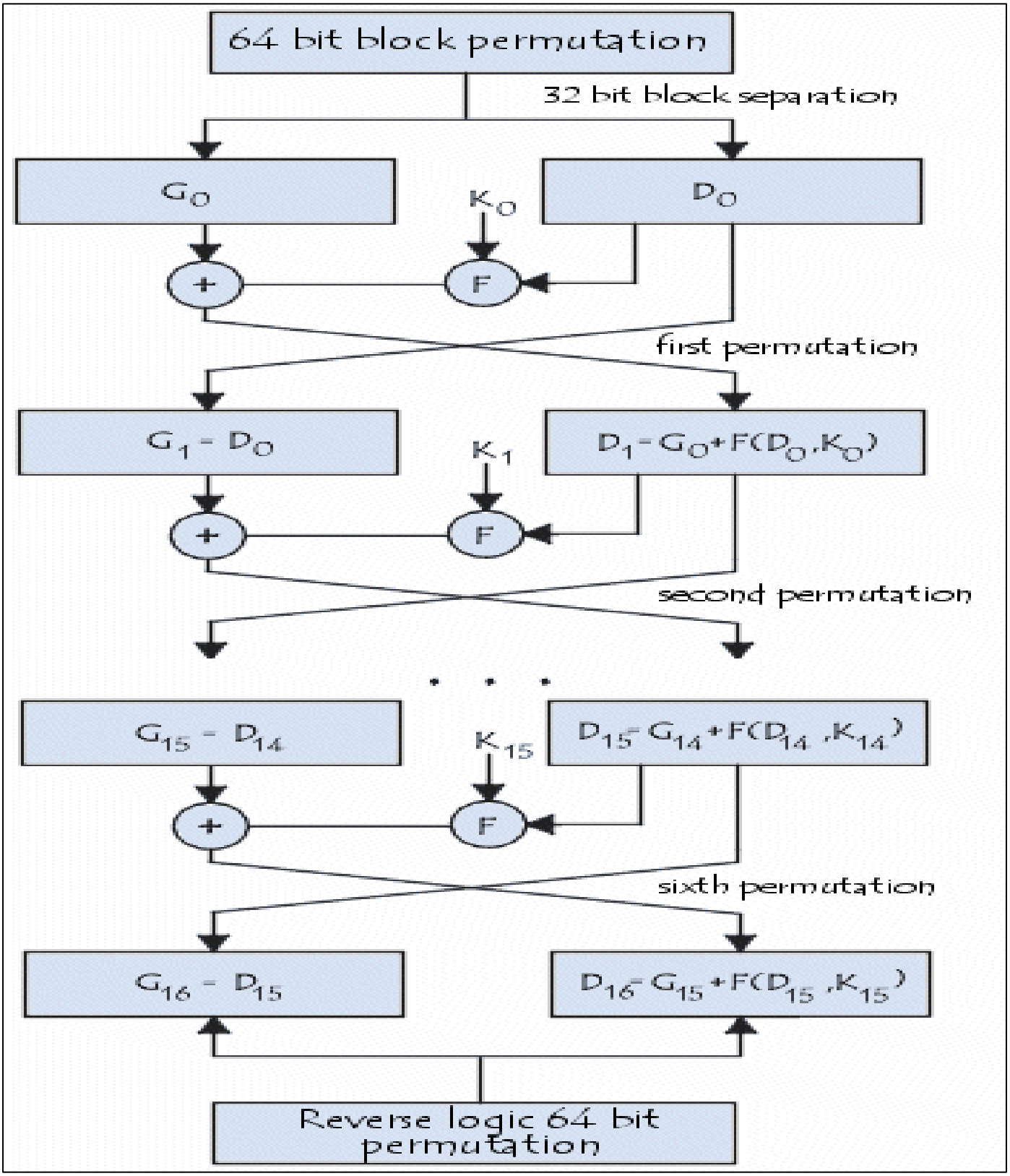

Fig 7 Block Diagram Showing Working of DES

- Permutation is applied to plain text.
- The parity bits are then eliminated by key substitution. Then following steps are performed:
- The two halves of the key are of the same size.
- Every component of the key rotates in accordance with the round being played.
- The key is then reduced from 56 bits to 48 bits by using a reduction recombination after the two halves have been recombined. The plain language of the session is encrypted using this 48-bit key.
- The values obtained by spinning each component of the key will be utilized to create the key for the next iteration.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

- The next step is to split the data block in half along its length.
- The data block's left portion is then permuted to extend its size by 48 bits.
- The data block's 48-bit permuted left portion then enters a function that performs an XOR computation between the key and the data block.
- The function's output is then passed provides input to the S-Box, which converts it to 32 bits, its actual size.
- This replaced output is then subjected to another permutation by P-Box.

D. Advance Encryption Standard (AES)

An improved cryptographic specification was created in 2001. AES is developed to provide data the highest level of protection. Hardware and software implementations of AES run swiftly. Instead of using DES, NSIT now uses AES. It is dependent on the size of the key used to carry out these operations how many rounds are needed to secure and retrieve the real data. The majority of 128-, 192-, and 256-bit keys have 10 rounds, 12 rounds, and 14 rounds, respectively.

The steps involved in an algorithm that protects data with a 128-bit block size

- The cypher key's size dictates how many rounds there are.
- The first-round key after initialization, the first-round key is appended to the state array.
- The identical procedure is used for the first rounds. Except for the last round, each round is identical.
- Immediately following that, the Final Round takes place.
- The result of the last round is the generated ciphertext.

➢ *Key General Methods*

- **Sub Word:** In order to create the output word, this operation substitutes the value stored in the S-box for the four-byte input word from the 4*4 matrix[48].
- **Rot Word:** The 4*4 matrix's bytes are cyclically shifted by this operation.
- **Rcon:** The final operation on the 4*4 matrix is XORing with the round constant Rcon, after Sub Word and Rot Word operations.

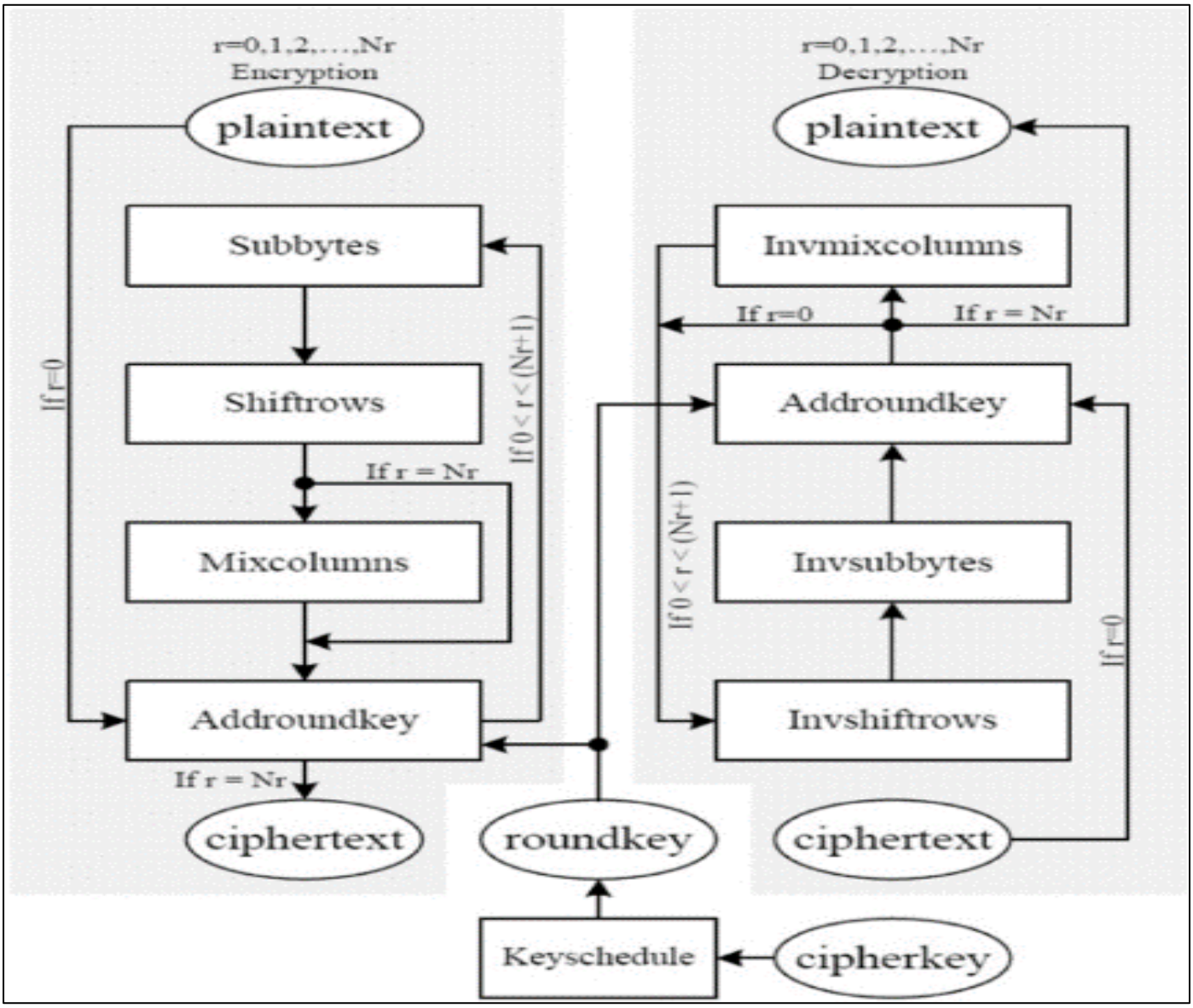

Fig 8 AES Algorithm

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

The AES (Advanced Encryption Standard) algorithm's structural process for encryption and decryption is shown in Figure 8. The encryption method uses several rounds of Sub Bytes, Shift Rows, Mix Columns, and Add Round Key, and equivalent inverse functions are used in the decryption path to reverse these operations. To provide safe and synchronized encryption and decryption cycles, the initial cypher key is used by a key scheduling module to generate round keys.

V. LITERATURE OF REVIEW

This literature review section focuses on current developments in quantum computing and cryptographic security, including distributed quantum operations in a variety of applications, modular quantum compilation, secure data transfer, real-time surveillance, and quantum reservoir computing.

Dsouza (2024) the surveillance system that integrates Mobile Net for real-time object detection, which employs robust encryption methods and utilizes a scalable and efficient system architecture. By dynamically adjusting security protocols based on real-time threats, the system enhances resilience and privacy. The societal benefits of this border surveillance system include the protection of critical infrastructure and improved national security. This review provides valuable insights into the most recent developments in border surveillance technology and emphasizes how DL and encryption might improve security protocols [49].

Jain et al. (2024) proposes a cryptographic model aimed at bolstering data security through advanced encryption techniques and secure data transmission protocols. The rapid evolution of digital technologies has transformed how they generate, transmit, and store data. However, this transformation has also exposed sensitive information to various security threats, underscoring the necessity for robust cryptographic frameworks to fortify data security. In order to protect data from unwanted access, guarantee data integrity, and provide secure communication channels, this research study presents a thorough cryptographic model that combines encryption, hash functions, and digital signatures [50].

Lohof et al. (2023) investigate the influence of quantum characteristics on the reservoir computer applicability of a system. Examine the connection between phase space dimension and reservoir entanglement. their results demonstrate that the proportion of the increasingly huge phase space utilized for computing rises with increasing entanglement. Also, go over ways to measure information that is dispersed over the network. Intentional or unintentional network symmetries have a big impact on the reservoir's memory capacity and dynamics. Finally, they point out the advantages and disadvantages of employing arrays of connected microcavities based on semiconductors for hybrid quantum-photonic reservoir computing solutions [51].

Ferrari et al. (2023) introduce a modular quantum compilation architecture for DQC that takes into account the constraints and characteristics of networks and devices. took into consideration different network topologies and quantum processors identified by heavy-hexagon coupling maps when developing and evaluating a quantum compiler with a few circuits of interest, such as the VQE and QFT circuits, using the proposed architecture. They also developed a remote scheduling method that can utilize both Tele Gate and Tele Data activities, and they assessed the results of using both or just Tele Gates [52].

Ahmed et al. (2022) examined how 5G edge computing combined with IoT networks helps with healthcare data transmission for remote medical treatment, looked into the security risks of unsecured data transmission, and finally proposed an end-to-end cryptographic security solution that begins at IoT sensor devices and is routed through SDN routers. Their proposed method provides end-to-end secure communication from the IoT device to the doctor's office via the SDN control plane and data plane in 5G edge computing, utilizing cryptographic security beginning at the IoT sensor. Positive outcomes have been obtained from the lab testing of a prototype using two-layer encrypted communication. Future eHealth security implementation in 5G and beyond networks will benefit from this insight [53].

Andrade et al. (2021) A description is given of a quantum walk protocol for distributed quantum computing in a quantum network. The protocol uses a quantum walk as a quantum control signal to carry out distributed quantum activities. examine an expansion of the discrete-time-introduced quantum walk model that accounts for the interaction between a quantum walker system in the network graph and quantum registers inside the network nodes. illustrate the universality of the networked quantum computing protocol by performing a distributed CNOT operation using the quantum walker system. Furthermore, it employs the protocol to resolve the quantum network's entanglement distribution issue [54].

Table I summarizes recent advancements in quantum computing and cryptographic security, highlighting innovative methods, key outcomes, and ongoing challenges across surveillance, secure transmission, distributed computing, and healthcare applications.

Table 1 Summary on Quantum Computing and Cryptographic Security

Reference	Focus On	Methods	Key Findings	Limitation / Future Gap	Challenges
D'Souza, (2024)	Real-time object detection in border surveillance using Mobile Net	Integration of Mobile Net with encryption, scalable architecture, and dynamic security protocols	Enhanced resilience and privacy; improved national security; protection of critical infrastructure	Requires further real-world deployment validation; adaptability in diverse terrains	Managing real-time data securely; balancing accuracy and speed

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

Jain et al. (2024)	Advanced cryptographic model for secure data transmission	Combining hash functions, digital signatures, and encryption algorithms	Enhanced communication security, secrecy, and data integrity	Needs testing on large-scale, heterogeneous networks	Combating evolving cyber threats; computational overhead
Lohof et al. (2023)	Quantum reservoir computing and system suitability	Analysis of entanglement, phase space dimension, network symmetries	High entanglement increases usable phase space; symmetries affect memory capacity	Experimental validation with physical systems is limited	Controlling quantum entanglement; implementing in hardware
Ferrari et al., (2023)	Distributed quantum computing via modular quantum compilation (DQC)	Quantum compiler for VQE/QFT circuits, network-aware scheduling (Tele Gate/Tele Data)	Effective compilation considering hardware/network constraints; strategy improves execution	Needs support for more circuit types and real-world network topologies	Limited current quantum hardware capability; scheduling complexity
Ahmed et al. (2022)	Secure eHealth data transmission in 5G-IoT networks	Two-layer encryption, SDN-based routing, IoT sensor-to-doctor path	Secured end-to-end communication; improved eHealth reliability	Prototype stage; limited scalability studies	Ensuring seamless encryption at low-latency; IoT device vulnerabilities
De Andrade et al., (2021)	Distributed quantum computing via quantum walks	Generalized coined quantum walk model; quantum control signals; distributed CNOT	Demonstrated universal distributed computing protocol and entanglement distribution	Real-world implementation and error correction not fully explored	Precision in quantum control; network synchronization

VI. CONCLUSION AND FUTURE WORK

Modern cryptography security faces a major threat as well as a revolutionary advance in quantum computing. RSA, ECC, and Diffie-Hellman are examples of conventional encryption systems that rely on two problems: discrete logarithms and integer factorization. These difficulties are computationally demanding for classical systems. However, due to exponential speedups offered by quantum algorithms such as Shor's and Grover's, these approaches are seriously vulnerable, putting the security and secrecy of global data networks at risk. One of the most important areas of study to combat these risks is PQC. Lattice-based, multivariate, and code-based cryptography are examples of intricate mathematical structures that PQC uses to thwart even quantum-level assaults. Numerous techniques, such as modular quantum compilation, quantum reservoir computing, and secure data transfer via the IoT, have the potential to influence next-generation security frameworks, as mentioned in the literature. The urgency and significance of this shift are highlighted by NIST's efforts to standardize PQC algorithms on a global scale.

Future research should concentrate on the widespread deployment of PQC systems in practical settings, particularly across low-latency and heterogeneous networks like 5G-IoT. Further investigation into hardware-based quantum security models, dynamic cryptographic protocols that can be adjusted to quantum threats, and dependable quantum control systems for dispersed contexts are also necessary. For the development of quantum-safe technologies to proceed more quickly and to guarantee a secure digital future, cooperation between researchers, legislators, and industry must be strengthened.

REFERENCES

[1]. S. Dixit, “The Impact of Quantum Computing on Cryptographic Security Protocols,” Adv. Nonlinear Var. Inequalities, vol. 27, no. 3, pp. 558–570, Aug. 2024, doi: 10.52783/anvi.v27.1419.

[2]. V. Prajapati, “Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions,” pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

[3]. S. Singh, “Enhancing Observability and Reliability in Wireless Networks with Service Mesh Technologies,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 1, 2025, doi: 10.48175/568.

[4]. S. Murri, S. Chinta, S. Jain, and T. Adimulam, “Advancing Cloud Data Architectures: A Deep Dive into Scalability, Security, and Intelligent Data Management for Next-Generation Applications,” Well Test. J., vol. 33, no. 2, pp. 619–644, 2024, [Online]. Available: https://welltestingjournal.com/index.php/WT/article/view/128

[5]. O. O. Amoo, E. O. Sodiya, U. J. Umoga, and A. Atadoga, “Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets,” Glob. J. Eng. Technol. Adv., vol. 18, no. 2, pp. 049–064, Feb. 2024, doi: 10.30574/gjeta.2024.18.2.0026.

[6]. S. Murri, “Data Security Challenges and Solutions in Big Data Cloud Environments,” Int. J. Curr. Eng. Technol., vol. 12, no. 6, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.11.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

[7]. M. Gopalsamy and K. B. Dastageer, "The Role of Ethical Hacking and AI in Proactive Cyber Defense : Current Approaches and Future Perspectives," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 2, 2025, doi: https://doi.org/10.5281/zenodo.14916984.
[8]. S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," J. Glob. Res. Electron. Commun., vol. 2, no. 2, pp. 1–7, 2025, doi: https://jgrec.info/index.php/jgrec.
[9]. V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," Int. Res. J., vol. 11, no. 12, pp. 74–82, 2024.
[10]. V. Pillai, "Anomaly Detection in Financial and Insurance Data-Systems," J. AI-Assisted Sci. Discov., vol. 4, no. 2, 2024.
[11]. A. K. Aftab Arif, Muhammad Ismaeel Khan, "An overview of cyber threats generated by AI," Int. J. Multidiscip. Sci. Arts, vol. 3, no. 4, pp. 67–76, 2024.
[12]. S. S. S. Neeli, "Securing and Managing Cloud Databases for Business - Critical Applications," J. Eng. Appl. Sci. Technol., vol. 7, no. 1, p. 6, 2025.
[13]. H. S. Chandu, "Advanced Methods for Verifying Memory Controllers in Modern Computing Systems," Int. J. Adv. Res. Sci. Commun. Technol., vol. 4, no. 2, pp. 377–388, 2024, doi: DOI: 10.48175/IJARSCT-19862.
[14]. K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, 2021, doi: DOI: 10.48175/IJARSCT-6268B.
[15]. J. L. Deepak Dasaratha Rao, Sairam Madasu, Srinivasa Rao Gunturu, Ceres D'britto, "Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study," Int. J. Recent Innov. Trends Comput. Commun., vol. 12, no. 1, 2024.
[16]. V. Pillai, "Enhancing Transparency and Understanding in AI Decision-Making Processes," irejournals, vol. 8, no. 1, p. 5, 2024.
[17]. V. Pillai, "Leveraging the power of Data Analysis in Automobile and Financial industries," Int. J. Eng. Comput. Sci., vol. 12, no. 12, 2023.
[18]. M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.
[19]. N. Abid, "Empowering Cybersecurity : Optimized Network Intrusion Detection Using Data Balancing and Advanced Machine Learning Models," TIJER, vol. 11, no. 12, 2024.
[20]. J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," Int. J. Res. Anal. Rev., vol. 8, no. 3, pp. 874–879, 2021.
[21]. M. I. Khan, A. Arif, and A. R. A. Khan, "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity," BIN Bull. Informatics, vol. 2, no. 2, pp. 248–261, 2024.
[22]. V. Prajapati, "Cloud-Based Database Management: Architecture, Security, challenges and solutions," J. Glob. Res. Electron. Commun., vol. 01, no. 1, pp. 07–13, 2025.
[23]. A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.
[24]. A. Gogineni, "Observability Driven Incident Management for Cloud-native Application Reliability," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 9, no. 2, 2021.
[25]. A. K. Bairwa, R. Yadav, D. D. Rao, K. Naidu, Y. H C, and S. Sharma, "Implications of Cyber-Physical Adversarial Attacks on Autonomous Systems," Int. J. Exp. Res. Rev., vol. 46, pp. 273–284, Dec. 2024, doi: 10.52756/ijerr.2024.v46.021.
[26]. N. Malali and S. R. Praveen Madugula, "Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 3, pp. 910–916, Mar. 2025, doi: 10.38124/ijisrt/25mar1287.
[27]. S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," J. Adv. Dev. Res., vol. 11, no. 1, p. 8, 2020.
[28]. S. Arora and S. R. Thota, "Automated Data Quality Assessment And Enhancement For Saas Based Data Applications," J. Emerg. Technol. Innov. Res., vol. 11, pp. i207–i218, 2024, doi: 10.6084/m9.jetir.JETIR2406822.
[29]. S. R. Thota, S. Arora, and S. Gupta, "Quantum-Inspired Data Processing for Big Data Analytics," in 2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE), 2024, pp. 502–508. doi: 10.1109/AECE62803.2024.10911758.
[30]. Filippo Di Giovanni, "Physical Principles Underpinning Quantum Computing," EE TIMES, 2024.
[31]. Godavari Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," Int. J. Adv. Res. Sci. Commun. Technol., vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.
[32]. A. V. Hazarika and M. Shah, "Distributed Quantum Computing Models: Study of Architectures and Models for the Distribution of Quantum Computing Tasks Across Multiple Quantum Nodes," Int. J. Sci. Res. Arch., vol. 13, no. 2, pp. 3719–3723, Dec. 2024, doi: 10.30574/ijsra.2024.13.2.2602.
[33]. Rajarshi Tarafdar, "AI-Powered Cybersecurity Threat Detection in Cloud," Int. J. Comput. Eng. Technol., p. 266, 2025.
[34]. S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," Int. J. Multidiscip. Res., vol. 3, no. 4, pp. 1–10, 2021.
[35]. R. Arel, "Classical vs. quantum computing: What are the differences?," TechTarget.
[36]. S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," Int. J.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may501

Innov. Res. Creat. Technol., vol. 8, no. 2, pp. 1–8, 2022.
[37]. A. R. A. K. Muhammad Ismaeel Khan, Aftab Arif, "The Most Recent Advances and Uses of AI in Cybersecurity," BULLET, vol. 3, no. 4, pp. 566–578, 2024.
[38]. V. Madiyala, "A Review of AR / VR Technologies in Simulation- Based Learning : Current Trends and Future Directions," vol. 1, no. 1, pp. 1–6, 2025.
[39]. N. P. K. Shukla, "Cybersecurity in The Era of Quantum Computing: Challenges and Future Directions," J. Emerg. Technol. Innov. Res., vol. 11, no. 9, pp. c843–c848, 2024.
[40]. M. S. Akaash Vishal Hazarika, "Serverless Architectures: Implications for Distributed System Design and Implementation," Int. J. Sci. Res., vol. 13, no. 12, pp. 1250–1253, 2024.
[41]. P. Piyush, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," J. Intell. Syst. Internet Things, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.
[42]. S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICIPTM59628.2024.10563348.
[43]. D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," Internet of Things, vol. 24, p. 100950, Dec. 2023, doi: 10.1016/j.iot.2023.100950.
[44]. N. Patel, "Quantum Cryptography In Healthcare Information Systems: Enhancing Security In Medical Data Storage And Communication," J. Emerg. Technol. Innov. Res., vol. 9, no. 8, pp. g193–g202, 2022.
[45]. M. S. S Shah, "Kubernetes in the Cloud: A Guide to Observability," DZone, 2025.
[46]. V. P. Shashikant Tank Kumar Mahendrabhai Shukla, Nimeshkumar Patel, "AI Based Cyber Security Data Analytic Device," pp. 414425–001, 2024.
[47]. M. S. Samarth Shah, "Deep Reinforcement Learning For Scalable Task Scheduling In Serverless Computing," Int. Res. J. Mod. Eng. Technol. Sci., vol. 3, no. 12, pp. 1845–1852, 2021, doi: DOI : https://www.doi.org/10.56726/IRJMETS17782.
[48]. H. Zodpe and A. Shaikh, "A Survey on Various Cryptanalytic Attacks on the AES Algorithm," Int. J. Next-Generation Comput., vol. 12, no. 2, pp. 115–123, 2021.
[49]. R. PM, H. Ravani, K. Aryan, S. R. Susikar, S. Vijay, and S. M. Dsouza, "Privacy-Preserving and Efficient Border Surveillance System using Advanced Deep Learning and Cryptographic Techniques," in 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Oct. 2024, pp. 733–736. doi: 10.1109/I-SMAC61858.2024.10714893.
[50]. A. Jain and H. Gupta, "A Cryptographic Model for the Enhancement of Data Security," in 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), IEEE, Mar. 2024, pp. 1–6. doi: 10.1109/ICRITO61523.2024.10522303.
[51]. F. Lohof, N. Gotting, and C. Gies, "Leveraging Quantum Dynamics for Physical Computing Applications," in Proceedings - 2023 IEEE International Conference on Quantum Computing and Engineering, QCE 2023, 2023. doi: 10.1109/QCE57702.2023.10262.
[52]. D. Ferrari, S. Carretta, and M. Amoretti, "A Modular Quantum Compilation Framework for Distributed Quantum Computing," IEEE Trans. Quantum Eng., 2023, doi: 10.1109/TQE.2023.3303935.
[53]. S. Ahmed, Z. Subah, and M. Z. Ali, "Cryptographic Data Security for IoT Healthcare in 5G and Beyond Networks," in 2022 IEEE Sensors, IEEE, Oct. 2022, pp. 1–4. doi: 10.1109/SENSORS52175.2022.9967208.
[54]. M. G. de Andrade, W. Dai, S. Guha, and D. Towsley, "A quantum walk control plane for distributed quantum computing in quantum networks," in 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), IEEE, Oct. 2021, pp. 313–323. doi: 10.1109/QCE52317.2021.00048.