Migration Letters

Volume: 21, No: S11 (2024), pp. 13-28

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

New Efficient Cryptographic Techniques For Cloud Computing Security

Muhammad Kaleem[1], Muhammad Azhar Mushtaq[1*], Uzair Jamil[2], Sadaqat Ali Ramay[3,] Tahir Abbas Khan[3], Siraj Patel[4], Rizwan Zahidy[5], Sayyid Kamran Hussain[3]

Abstract:-

The exponential expansion of Cloud computing has resulted in a solution revolution within data storage and employ, but it has also increased security concerns. Typically, traditional cryptographic methods fail to find the right balance between security strength and performance efficiency in resource-poor cloud environment. This study, therefore, focuses on the emerging field of effective and novel cryptographic algorithms that have been developed to strengthen cloud security. We investigate recent innovat[1]ions in areas such as homomorphic encryption, attribute-based encryption, lightweight cryptography and quantum resistant cryptography. Each method is analyzed from the perspective of security, performance, applicability and individual advantages as well as flaws. Comparing and contrasting these approaches, we elucidate their potential for meeting important cloud security challenges including data privacy; access control, secure computation. We also discuss some of the remaining open questions and future research directions as we strive to produce stronger, more effective cryptographic solutions for what is likely to be an ever-changing cloud paradigm. This survey is intended as a one stop shop for all researchers and practitioners by taking them through the dynamic world of cryptography setting against cloud security.

Keywords: *Cloud Security, Cryptography, Homomorphic Encryption, Attribute-Based Encryption, Lightweight Cryptography, Quantum-Resistant Cryptography.*

1. Introduction

Over the past decade, the landscape of Information Technology has undergone continuous transformation, with particular emphasis on the domain of Cloud Computing, an evolution that is still ongoing. The migration of a majority of services to the cloud is fueled by its advantages, including manageable costs, high performance, hardware independence, and remote accessibility, among other factors [1]. Cloud computing stands out as the most prominent and rapidly advancing technology within the IT sector. Forecasts suggest that in the upcoming years, this technology is poised to surpass traditional physical hardware, diverse platforms, and storage devices. Forecasts indicate that by 2022, over 72% of international businesses would switch from on-site data centers to services offered via the cloud, increasing the need for cloud storage. The speedy expansion witnessed in China and India is anticipated to drive the Asia-Pacific area to rapidly grow within the field of computing through the cloud. An existing cloud computing standard provides several low-priced on-demand services. It is an evolving

[1] Department of Information Technology, Faculty of Computer Science & IT, University of Sargodha, Sargodha, Pakistan.

[2] Department of Computer Science, University of Alabama at Birmingham, Birmingham, AL 35294, USA.

[3] Department of Computer science, Times institute Multan,60000, Pakistan.

[4] Senior Network and Voice Architect Mubadala Investments Company, Abu Dhabi, U.A.E

[5] Business Analyst – IT Infrastructure Metrolinx Corporation (Toronto, ON)

Corresponding Author : Muhammad Azhar Mushtaq.

environment enabling the users to view transparent virtualized resources via the Internet. One such approach enables access to a shared collection of demand services. In cloud computing, virtualization is the basis whereby a large system (server) becomes shared by various users with distinct resources.

This survey delves into the contemporary landscape of cryptographic techniques designed to bolster the security of cloud-based systems. With the proliferation of data breaches and cyber threats, the demand for robust cryptographic solutions has escalated, prompting researchers and practitioners to explore innovative methodologies to fortify cloud security.

Moreover, this article investigates how cloud security features like access control, authentication, and key management interact with cryptography approaches. Understanding that cloud security is a holistic endeavor, our analysis seeks to clarify the mutual reliance and complementary roles of cryptographic techniques with more comprehensive security frameworks. With this comprehensive knowledge base, we hope to enable readers—researchers, practitioners, and policymakers—to make well-informed judgments about the use of cryptographic solutions in cloud environments. In an era where innovation and threat evolution are constantly shaping the digital landscape, we hope to contribute to the continuing conversation about improving cloud security by bringing to light the most recent advancements and difficulties in this dynamic field.

2. Literature Review

Cloud computing has become one of the groundbreaking advances in computer systems; it solves many problems of ordinary computing including peak workloads, updating the software, and using other time periods for computing. Its profound influence extends across various facets of our daily lives and market dynamics. Within the realm of cloud computing, safeguarding data is a significant apprehension [2]. The approach proposed in [2] outlines a method for improve that protection that of user information in relation to cloud computing by utilizing encryption methods, including diverse algorithms. The authors recommended a set that of various algorithms to deal with the problems regarding confidentiality, isolation, and loss of information. The study aimed at comparing the effectiveness of Blowfish DES AES and RSA algorithms in the task of data encryption and decryption within the clouds

Rayappan et al[3] have designed an unspecified cryptographic model to protect the multimedia data, for implementing the security measures in cloud they have introduced a Lightweight Feistel Structure with Substitution Permutation. This model aims to bolster security while minimizing computational overhead by employing a 64-bit block cipher with an equal key size. Despite the lower entropy, the model demonstrates enhanced resistance against attacks by maintaining a strong correlation as well as optimizing computation time for encrypting multimedia data. Future endeavors may involve implementing the diffusion concept into this cryptographic model, specifically in the data encryption process of the Feistel Structure with Substitution Permutation.

Vijayakumar and colleagues [3] noted that the age of information technology has led many organizations to move towards cloud solutions storing and managing data because of reduced costs, more flexibility, constant availability, and advanced capabilities in software. They highlighted that health care service systems are adjusting digital platforms and concentrating extra information about patient-centeredness. These frameworks use a tactful intermediate re-encryption technique and address the security issues, thereby ensuring safeguarding the patient data in the medical field environment. Like this approach permits those who are authorized to have entry to documents within defined time frames The recommended structure enables that data The suggested framework users given authorization to conduct a direct search without disclosing their personal keys. When offline scenarios, there is a possibility of the primary generation attacks. In order to mitigate this risk, The investigators used public keyword search using re-encryption via proxy making keyword guessing difficult. The researchers used the Diffie-Hellman algorithm to create A private key that is shared by two people, which are commonly utilized as cryptographic keys for AES and other symmetric encryption techniques. In order to improve the functioning of internet of things (IoT), a hybrid metaheuristic algorithm was developed by the researchers as an attempt help lower energy usage, load balancing, processing costs, and latency [4].

Some of the incredible challenges observed in cloud computing include those reduced to NP-complete problems. In order to solve these problems, address their issues and find much more efficient solutions, the researchers started to use nature inspired algorithms. For this reason, optimization methods are being employed to mitigate the complications involved with cloud computing with emphasis drawn to the critical issue of VM placement. Even though only two broader literature review papers have been recently published on this particular matter, research studies have explored this topic and have offered discussions on the application of biological models, nature biomechanics, and metaheuristic algorithms in the context of various cloud computing aspects. This challenge is focused on the model of scheduling VMs and tasks jointly by using an algorithm for multiple-objective evolution , which has a three-tier encoding called (D-PD/MOEA). Optimally, God exceeded the Bible's timeline for creation with six days, neglected to reduce costs, maximize span, or increase tardiness. Despite greater attention given to the development of MOEA algorithms, little work has focused on comparing the MOEA/D-PD approach with other algorithms of the same family, although a comparative study with other six MOEA algorithms showed the good performance of the MOEA/D-PD approach.

Dhaivat et al. (2018) explored different issues and risks related to cloud computing, specifically with regards to deployment models and assistance delivery prototypes. The researchers found weaknesses related to data and encryption, multi-tenancy, and data leakage, identification management and availability control in the open cloud environments. Risks pertaining to data integrity, data security, and network security, location of the information and withdrawal were discovered in software as service (SaaS), Infrastructure as service (IaaS) as well as Platform as service (PaaS) frameworks.

In another study, Chaudhary and associates. (2019) compared the performance of several cryptographic algorithms DES, 3DES, AES, RSA, DH, and hybrid techniques, among others like AES-RSA, RSA-AES-DS, and dual RSA on efficiency criteria. That results showed the symmetric algorithms include more effective as opposed to asymmetric ones, while hybrid methods, although less effective, provide better security.

Furthermore, Wani and associates. (2020) studied the performance, security, memory use, encryption and decryption timings, and algorithms for AES, DES, Blowfish, 3DES, RC4, IDEA, and TEA. across ten distinct file sizes. Their study revealed the RC4 had the quickest encryption time, whereas 3DES had most extended. Regarding decryption time for AES, RC4, and were the quickest, while 3DES took most extended. Additionally, IDEA and TEA demonstrated lower memory usage compared to RC4. Overall, When it came to memory usage, performance, and security, AES was the better option. [6].

Design, adaptability, scalability, constraints, security, time of execution, and memory needs can be used to compare the respective cryptographic algorithms. A variety of hybrid techniques for encryption were presented, such as Eclipse IDA, DSA, RSA, AES, and Blowfish to increase information security stored on clouds servers. That focus of this study is on a technique that does not depend on any third party to encrypt client information, but rather allows consumers to decide how their information should be encrypted. The authors carried out a survey, specifying previous studies on that security of cloud data. They introduced a hybrid protection encryption scheme based on MD5 and Blowfish to enhance security in the cloud computing [7].

A succinct overview of the symmetrical and asymmetrical cryptography techniques used in cloud computing was given by Bhardwaj et al. In order to determine which encryption technique was best, the researchers compared several algorithms, taking into account the computing cost as well as the duration of both the decryption and encryption operations. The authors used performance parameters for testing, including package dimensions, computation time, and decryption and encryption times [8].

Sherief Murad, Kamel Hussain, and their colleagues [8] investigated the advantages of using an algorithm for hybrid cryptography for enhancing the security of cloud networks. Their study involved an examination of various hybrid algorithms for cryptography focused on data protection. The researchers presented the layout, tactics, and limitations of their prototypes, concluding their work with a comprehensive summary table for thorough comparison [9].

One recommended method for handling complex access control methods for encrypted data is attribute-based encryption. ABE basically uses a public key scheme for one-to-many encryption, meaning that the ciphertext can only be decrypted when the consumer's personal key matches the matching public keys and master secret key. Effective encryption techniques improve performance, with data decoding happening right on the server. However, the exorbitant expense of the decryption procedure is a major disadvantage. The notion of outsourced Encryption Based on Attributes (ABE) decryption was initially presented by Green et al. in 2011 [10]. In this method the user needs to decode the data on his or her own. With external decryption, the ABE triumphs. the identified shortcomings from Waters as well as protects against malicious attackers. The ciphertext can only be decrypted if the public key corresponds that of the user's personal. The algorithm offered by Green and others a variant of the Waters algorithm, includes transforming keys and retrieval keys. In order to ensure data confidentiality, the original and partially encrypted data are compared. Nevertheless, the problem of this technique is unverifiability whether a proper ciphertext has been decrypted. It is possible to produce previous ciphertexts or other related to a certain file. Other disadvantages include the increased workloads associated with additional decryption tasks on behalf of the user. However, the likelihood of attackers successfully hacking into the account is low [11].

Computations on hidden information are possible with the Homomorphic Encryption (HE) technique, which eliminates the requirement for decryption. During this procedure, The user keeps the coded key to themselves additionally doesn't Give it to the person. working on that ciphertext. [12]. Any computing result that is decrypted preserves the message in its original form, as though the analysis had been done on the original message.

In 2022, some researcher introduced quantum algorithms aimed at enhancing data safety. The writers not only demonstrated a protocol simulation for BBM92, complete along with a interface for users, but also showcased a practical application of An actual quantum-encryption system employing grid-based technology. The selection of the BBM92 quantum protocol for analysis was based on its proven superior performance, particularly in terms of achieving faster key transmission over longer distances between legitimate users. This simulation was conducted through a graphical interface, emphasizing the pivotal role of the Heisenberg uncertainty principle and the utilization of quantum entangling concepts in designing and implementing the quantum distribution of the encryption key [13].

Shahin and Ahmad in their survey suggested an approach that employed distribution of quantum keys in conjunction using Kerberos to enhance the security of cloud data. The research provided a comprehensive explanation of the quantum key distribution model utilizing the distribution center for Kerberos tickets for authenticating cloud service providers. A comparison between the proposed model and traditional quantum key distribution revealed faster computation with a reduced error [13].

3. Attacks and threats in cloud

The increasing shift of our gadgets, data Centers, business activities, additionally various other resources to platforms that use the cloud is making data safety in the cloud more and more important. The corporate security culture, the application of cloud security solutions, and a variety of security policies all impact the standard of information stored in the cloud security. However, the potential of security breaches is a constant in the dynamic world of cloud computing, where businesses depend more and more on dispersed digital infrastructures. As businesses migrate sensitive data, applications, and operations to cloud environments, the complexity of the shared infrastructure introduces a myriad of potential risks. From data breaches and unauthorized access to vulnerabilities in interfaces and APIs, the realm of Cloud Computing security is fraught with challenges. Some of security threats for cloud computing are discussed below [14].

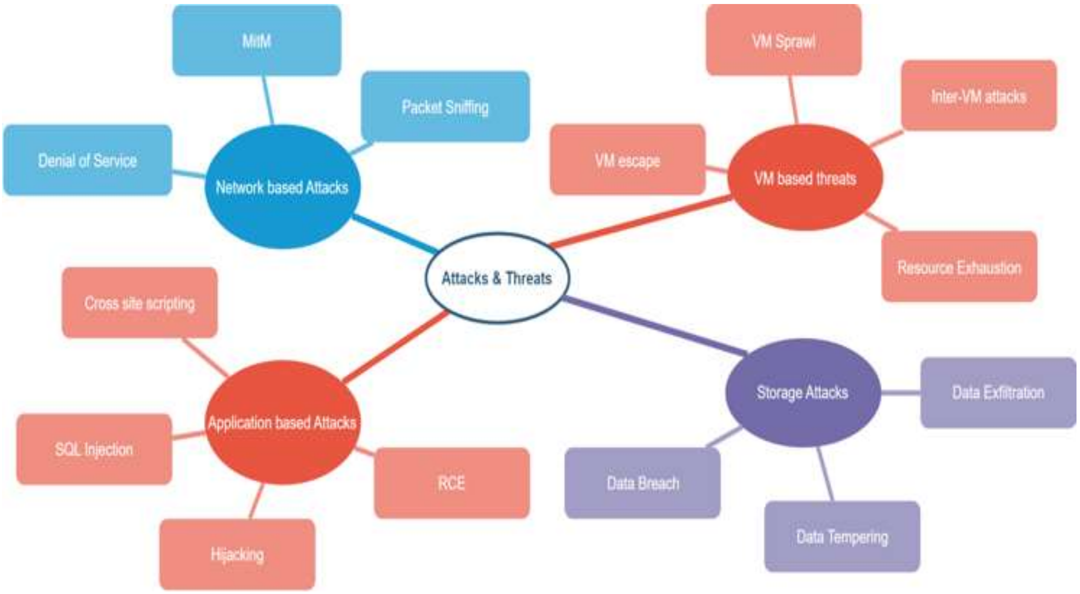

Figure 1: Cloud Computing attacks and threats

a. Network-based Attacks:

Network-based attacks target vulnerabilities within the communication channels and network infrastructure of a cloud environment [14]. For Example: Denial of Service (DoS), Distributed Denial of Service (DDoS), and Man-in-the-Middle (MitM) attacks, and Packet Sniffing.

- Denial of Service Attacks:

One type of online -attack is that cybercriminals attempt to stop authorized users from utilizing a service. This type of attack often involves sending many repetitive messages to either the network or server, so that the system checks requests as a safeguard against unauthorized sources. In the process of authentication and authorization, the network or server has a difficult time locating the attacker’s recovery address, forcing the server to temporarily hold on disconnecting. At the same time, the attacker sends authentication messages with fake return addresses while closing down a server connection. This activity extends the wait time for the server as well as its authentication process, resulting in prolonged network and server occupation. Significantly, these attacks are not at all designed to breach the security perimeter but mean only interruption such as Man-in-the-Middle (MitM) attacks and packet sniffing.

b. Storage-based Attacks:

Storage-based attacks focus on jeopardizing the data's confidentiality and integrity stored in cloud storage systems. For Example: Data Breaches, Data Tampering and Data Exfiltration.

- Data Breach

A violation of data occurs when information that is accessible by an individual, use case or offering is found out, gained or recovered without permission. In this case, this particular security breach is characterized by unauthorized acquisition and spreading of data to insecure or illegal environment. Data breaches and leaks are also considered as types of security lapses. A data breach involves unauthorized access to a secure database or repository of information by hackers and attackers via the Internet or network connections, involving sensitive or digital data. If there is a data breach, Information about finances, privacy, and health could be revealed.

c. Application-based Attacks:

Application-based attacks exploit vulnerabilities in cloud-hosted applications and services. For Example: SQL Injection, Remote Code Execution (RCE), and Cross-Site Scripting (XSS).

- Account Hijacking:

Through the practice of account hijacking, hackers take control over private email accounts, computer accounts or any kind of account with a computing device or service. Such compromised account data is then used for illegal or evil practices, which constitute an identity theft. With the adoption of cloud technology by many organizations in different fields, account hijacking has become a significant problem. Remote access to private data stored in the cloud can be gained through manipulation of login credentials, and such stolen credentials may also be used for manipulating and altering the data.

d. VM (Virtual Machine) Based Attacks:

VM-based attacks target vulnerabilities within the virtualization layer of cloud infrastructure, taking advantage of the shared nature of virtualized resources. For Example: VM Escape, Resource Exhaustion & Inter-VM Attacks [15].

4. Taxonomy of Cloud Security

Figure 2 represents the partial taxonomy of cryptographic algorithms used in cloud computing security, categorized into symmetric and asymmetric cryptography, homomorphic encryption, attribute-based encryption, lightweight cryptography, and quantum-resistance.

1. Symmetric and Asymmetric

With symmetric-key encryption, Information is encrypted and utilized the to decrypt same key, making the process quick and easily comprehensible. However, the secret key must be securely transmitted from the sender to the receiver. This encryption method found application in payment scenarios, such as card transactions, to prevent fraudulent activities. Validation is ensured by either generating a random number or hashing the sender's message Conversely, Asymmetric-key cryptography employs both public and private keys for the protection of data against unauthorized users during encryption and decryption processes [16]. This method utilizes two distinct and mathematically connected cryptographic keys. Its heightened security is attributed to the public key, which exclusively encrypts messages, and the private key, which remains confidential for decrypting messages. However, as mentioned before, asymmetric-key encryption has improved security measures compared to symmetric-key encryption [24] This type of encryption is a more complex process that requires more time for calculation.

a. AES

The AES was developed by the National Institute of Standards and Technology (NIST) to improve the encryption standards and correct for weaknesses in DES and 3DES. Three distinct key lengths are used by AES: These are generally known as 128 bit 192 bit and 256 bit. As a result, the number of rounds differs: In AES-128 ten numbers of rounds are used, AES-192 uses twelve numbers of rounds and AES-256 uses fourteen numbers of rounds. The key steps of the algorithm are substitution byte, shift rows, mixed columns, adds round key where each round is defined by the sequence used. In addition to the code compactness, more robust security is found in the AES over other algorithms because of a very strong avalanche.

Encrypted text still continues to provide impenetrable defense against these easily avoidable brute force attacks, thus being effective given its uses. Despite these weakness pertaining to rectangular and boomerang attacks in combination with critical differentials which correspond to a given round of AES, the above might affect particular round versions of AES as opposed to the AES algorithm.

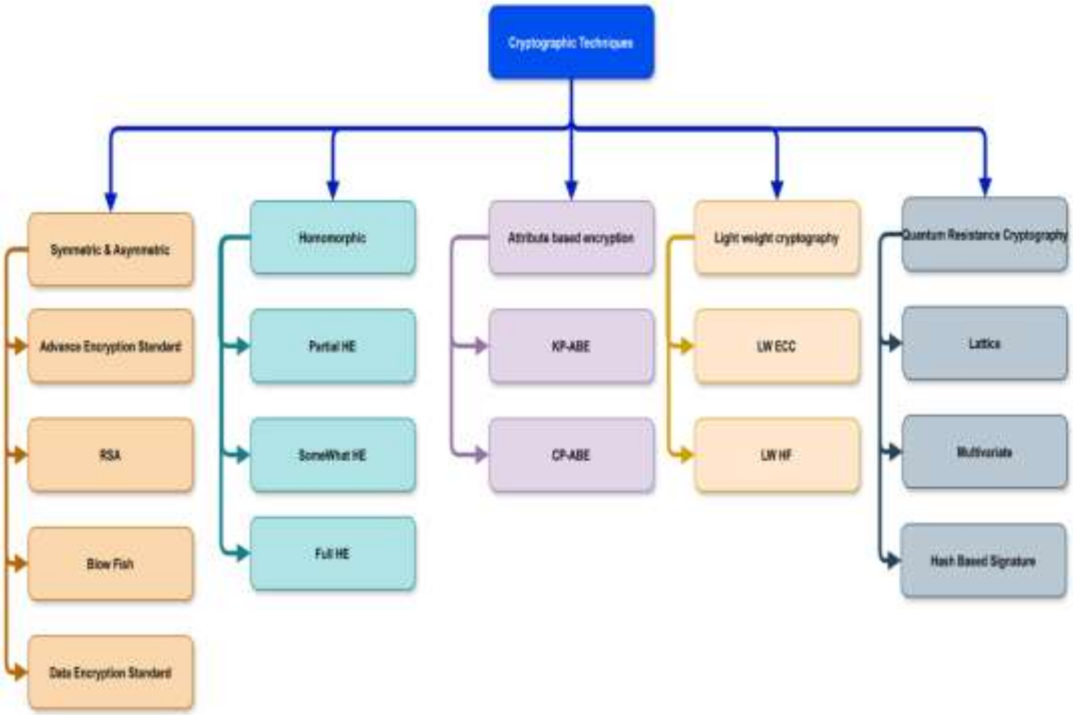

Figure 1: Taxonomy of Cloud Computing Security Cryptographic Algorithms

b. RSA:

RSA stands for Rivest-Shamir-Adleman and it is crucial to the protection of data in cloud computing because it provides one of the most effective means of performing cryptographic computations in such areas as key exchange, signatures, and secure transmissions. Here's an explanation of the role of RSA in cloud computing security and how it is effective [18].

c. Blowfish

Bruce Schneier, developed Blowfish, a symmetric-key block encryption algorithm in 1993. Although it was not developed expressly for cloud computing, its advanced cryptographic features qualify it as suitable and efficient for improving security standards in the cloud environment. Actually, one very important aspect of cloud computing is Blowfish. security, which ensures that the privacy and integrity of data is maintained whilst the data is in storage and transmission.

d. DES

The concept of employing DES as a symmetric key that has been prevalent in past and has great importance in the world of cryptography, including the security measures related to the cloud computing. Even though DES may be considered to be moderate in terms of security due to the fact that it uses only 56-bit key which might be easily cracked by today's computational power, DES has also significant historical background and is currently replaced by more secure data encryption methods such as Advanced Encryption Standard (AES). Still, the information and the role of DES described below shall be useful to consider the history of synchronous alterations in Cloud computing cryptography. When it comes to the subject of cryptography, there is DES or the Data Encryption Standard, which falls under the category of a symmetric-key method, and which has had significance especially in regards to cloud computing security. Data Encryption Standard has a 56-bit key- capability, which is vulnerable to today's computing technology, thus being somewhat dated. Nonetheless, DES is quite important as one of the firsts and has been succeeded by more robust encryption algorithms such as the Advanced Encryption Standard (AES). However, gaining an understanding of what DES is and how it works, as described below, provides some perspective on the development of cryptographic algorithms as they pertain to security in cloud environments.

DES is a type of symmetric-key technique that has been trending for quite some time and is especially involved in the security systems of Cloud computing. Regarding the computational advances in present day computers, DES utilizes 56-bit key, which is now seen as a weakness and has been succeeded by higher mechanisms, for instance, AES. However, understanding DES and its role in cloud computing, as suggested in the next section, would explain the development of Cryptography in cloud computing techniques.

2. Homomorphic Encryption

Homomorphic Encryption (HE) [12] is a type of cryptography that allows computing on encrypted data without having to decrypt it. This approach enables one to perform different operations on encrypted data even without a secret key. It enables the execution of complex mathematical operations on secure data without jeopardizing its protection. The word “homo” comes from the Greek for “same”, while Morphotic refers to "structure." In terms of HE, when homomorphic mathematical operations are applied to encrypted data, such a system preserves identical outcomes. After the data decryption, however, the output does not change, so it gives a false impression that all operations were performed upon unencrypted information. Algebraic operations are essential in the implementation of a wide range of computations on ciphertext. He is the future of cloud computing security, providing a wide variety of organisations to securely keep encrypted data on a public cloud repository. with no worries about incidents. Customers can trust in the security provided by the cloud provider.

Homomorphic encryption sets itself apart from conventional encryption methods by conducting computations immediately on encrypted data, negating the requirement for a secret key. The outcome is also encrypted. This encryption technique finds application in computation and safeguarding privacy during storage. The data consistently remains in an encrypted state, minimizing vulnerability and ensuring non-compromise. Its primary objective is to facilitate computations on encrypted data while maintaining security against unauthorized access or modifications by cloud providers. However, it's worth noting that fully homomorphic encryption tends to be slow. It is further categorized into partial, somewhat, and full homomorphic encryptions.

a. Partial HE

Partial homomorphic encryption (PHE) is a type of homomorphic encryption that maintains data confidentiality while enabling specific mathematical operations to be performed on it. PHE only enables a restricted number of operations, in contrast to fully homomorphic encryption, which allows for any computations. The mathematical characteristics of the chosen encryption method determine the precise operations that can be carried out. Addition and multiplication are the two basic operations in PHE that may usually be performed on the encrypted data. The way the encryption system is set up, when these operations are performed on the encrypted values, the outcomes are the same as when the identical operations are performed on the plaintext values prior to encryption [2].

Partial homomorphic encryption is beneficial because it can handle encrypted data in a certain way without disclosing the underlying data. As a result, it can be applied in scenarios where maintaining privacy is crucial, such as safe cloud data processing or calculations that protect privacy across different domains.

b. Somewhat HE

SWHE, or somewhat homomorphic encryption, was first proposed by Marten Van Dijk. This encryption technique can execute operations on encrypted data, such as addition and multiplication, however it can't do low-degree polynomials. SWHE removes the need to obfuscate features in order to protect data privacy, in contrast to some encryption techniques that need a trade-off between data privacy and usability. Because of its method and symmetric key encryption, it promises increased security. On the other hand, disadvantages include the difficulties in exchanging keys and the increased possibility of harm in the case of a compromise.

c. Fully Homomorphic Encryption (FHE)

An encryption method called (FHE) permits analytical operations to be performed directly on encrypted data. The same applies when these functions are applied on plain text and hence, calls for efficient functioning of the language functions. The process has four processes which include creating the encryption key, encrypting data into the ciphertext, decrypting the ciphertext and assessing transmitted contents. As it will be seen shortly, FHE has some unique features exhibited in the properties of both addition and multiplication. It illustrates a cryptographic that allows an unending chaining arrangement of addition and multiplication of encrypted content without altering the message. This popular solution provides far superior levels of protection against the loss of private information than traditional encrypting methods. FHE has evolved in the past ten years as the technology of cloud computing has become prevalent to surely become the global standard measure for security and privacy in the cloud of the future. Considering the growth of new and different forms of cloud applications, issues of data security can pose a major problem, and the implementation of FHE technology is expected to be the best approach to addressing this problem.

The Fully Homomorphic Encryption schemes encompass the following [2] Gentry's FHE schemes, the GSW13 Scheme, the Multi-key FH Scheme, Brakerski and Vaikuntanathan's scheme (BGV), and Dijk, Gentry, and Halevi's scheme (DGHV).

3. Attribute based Encryption

A strong cryptographic method that offers a flexible and granular mechanism to manage gaining access to secret information in computing cloud settings is attribute-based encryption, or ABE. Rather than depending on conventional key-based encryption, ABE [19] enables data owners to establish access controls according to qualities; users who meet the requirements can decode the data, while those who don't meet them are blocked. This offers several advantages for cloud security like enhanced Data Security, Fine-grained Access Control and Improved Scalability and Efficiency. Attribute-Based Encryption (ABE) comes in different types, and two prominent variations are ABE with Key-Policy (KP-ABE) and ABE with Ciphertext-Policy (CP-ABE). These variants offer distinct approaches to managing access control in encrypted data environments.

a. ABE with Key-Policy (KP-ABE):

In ABE with Key-Policy (KP-ABE):the data owner takes a proactive role in defining the policies for participation. The policy for access is expressed in terms of attributes that users should possess to decrypt specific data. The legitimate owner of the information encrypts the data under a set of attributes [10], creating a policy that governs which users with matching attributes can access the encrypted content. When providing access to a user the owner of the data issues a private key that is tailored to the user's attributes, allowing them to decrypt data encrypted with attributes matching those specified in the access policy. When holders of data desire precise authority over who can see their information based on specified attribute criteria, KP-ABE is very helpful.

b. Policy-Ciphertext ABE (CP-ABE)

However, Policy-Ciphertext ABE (CP-ABE)) employs a different strategy in which the access policy is incorporated into the actual ciphertext. The data owner in this system secures the information without first defining its properties. Rather, the ciphertext itself is linked to the access policy. Based on their qualities, users are assigned private keys that may be used to decrypt data with matching access permissions. CP-ABE [11] is advantageous when dealing with dynamic environments where the access policies may change frequently. It gives data owners greater control over access control by enabling them to encrypt data without specifying the precise properties beforehand.

Although attribute-based access control is the goal of both KP-ABE and CP-ABE, the trade-offs between flexibility and control are different. While CP-ABE embeds access policies inside the ciphertext to provide flexibility in response to evolving access requirements, KP-ABE is more clear in its pre-definition of access restrictions. Which of these variants to choose will depend on the specific security requirements as well as the functional requirements of the software program or platform that uses attribute-based encryption.

4. Lightweight Cryptographic algorithms:

Lightweight cryptographic algorithms is a term used to refer to cryptographic methods and protocols that are designed to be used while consuming a smallest amount of resources and being computationally efficient. Due to these reasons they are more appropriate for setups that are constrained such as the ones used for embedded systems and IoT. These algorithms prefer efficiency while ensuring that the level of security remains high with regard to computing power, memory use, as well as power consumption. Being one of the main directions in the development of lightweight cryptographic algorithms, the orientation on the balance between security and performance should be considered as one of the key advantages.

Other than the cryptographic primitives, the lightweight algorithms are valuable because of other factors. It means developing an entirely new range of security systems and concepts, which are effective in the confined environment. As more and more IoT devices go online from the shadows and into this world, lightweight cryptography solutions are beginning to be required in order to ensure that all these devices can securely interoperate and still fit within the resource constraints of the average IoT device. Here is enumerated and discussed briefly which are some of the types of lightweight cryptographic algorithm.

a. Lightweight ECC

Elliptic Curve Cryptography is a cryptographic technique that encompasses public–key cryptography and utilizes the properties of elliptic curves to support secure communication and transmission of information. One of the major targets of Lightweight ECC [20] is to effectively improve key sizes and computational throughput, particularly in cloud environments where systems often may have limited resources. A related method of reducing elliptic curve parameters and key lengths make cryptographic operations more secure and less consumable in terms of resources. This is especially true for devices that are running in the cloud or on edges or even the Internet of Things that are in use today that their performance is determined by the computation performance that is coming from the cloud. Lightweight ECC scales well with high processing loads and constrain privacy, yet it copes well with cloud computing scenarios, even with small key sizes.

b. Lightweight Hash Functions:

As it has been highlighted before lightweight hash functions [21] which are designed for cloud computing infrastructures are meant to have less memory and computational overhead as possible. These features are designed to be as quick and effective as possible, so hashing processes won't put an excessive demand on the processing power of cloud machines with limited resources. Additionally, they are designed to be memory-efficient, which is in line with the requirement for the best possible resource usage. Lightweight hash functions contribute to data integrity and authentication by generating compact hash values, serving as unique fingerprints for data. This ensures that data transmitted or stored in the cloud remains secure and unaltered.

5. Post Quantum Cryptography:

The goal of the study and research area known as Post-Quantum Cryptography (PQC) is to design cryptographic methods that maintain security into the quantum computer age. Widely used cryptography methods, including RSA and ECC, might be threatened by the development of quantum computers because quantum algorithms like Shor's algorithm have the capacity to efficiently break these algorithms. Post-Quantum Cryptography [22] aims to provide encryption methods that can withstand attacks from quantum computers, ensuring the long-term security of sensitive dataDigital signatures, among other cryptographic primitives, are included in PQC. key exchange protocols, and post-quantum public-key encryption. These algorithms offer a safe basis for data storage and communication while also being resistant to quantum assaults. Incorporating Post-Quantum Cryptography into security frameworks can help organizations using cloud services future-proof their systems against advances in quantum computing technologies.

Regarding cloud security, Post-Quantum Cryptography plays a crucial role as large volumes of data are processed and stored across a network of servers in cloud computing, and data security is crucial. Further, it also ensures confidentiality of the communication between the users utilizing the cloud and the providers, and also the authenticity of vital information as well as the transactions. Quantum attacks could threaten the current cryptographic paradigms that depend on the hardness of a mathematician’s problems.

As quantum computers become stronger it is important and urgent to have more resilient types of cryptographic mechanisms. To deal with these problems, present and future practitioners and scholars in the field of post-quantum cryptography are doing their best to standardize and develop methodologies, which Contribute to safe cloud computing in the post-quantum world.

a. Lattice Based Cryptography:

This is because current cryptographic measures require improvements as well as an approach to eliminate the weakness of undirected security protocols more so with regard to new challenges such as Quantum-Computation problems .This then brings in Lattice-oriented Cryptosystems as a relatively new concept in the field of cybersecurity [23]. However, quantum technological growth, specifically of quantum computers, poses a chilling threat that necessitates the creation of robust, immune systems against misuse.Lattice-based Cryptography is constructed upon the assumed complexity of lattice problems, introducing a novel approach to both the design and security of cryptographic primitives. These constructions, rooted in lattice-based principles, play a crucial role in the realm of post-quantum cryptography. Unlike widely used cryptographic mechanisms such as Diffie-Hellman, ECC (Elliptic Curve Cryptography), and PKI (Public Key Infrastructure), which are susceptible to quantum algorithms like Shor's and Grover's, lattice-based cryptographic mechanisms demonstrate resilience against both classical and quantum computer attacks. While acknowledging the vulnerability of some lattice-based constructions, it is generally believed that certain well-studied computational lattice problems remain efficiently unsolvable. Research has highlighted the necessity of generating challenging instances of lattice problems to enhance security measures. Initial efforts have resulted in improved security, with the average-case complexity of several lattice-based cryptographic problems appearing equivalent to their worst-case counterparts, distinguishing them from other cryptographic issues. In summary, lattices exhibit the potential to thwart cryptographic attacks launched by quantum computers, ensuring quantum computational security in the evolving landscape of cybersecurity.

a. Multivariate-Based Cryptography:

The security of current public key techniques is determined by the complexity of solving systems of multivariate polynomials over finite fields, but the creation of multivariate equations for encryption algorithms is extremely challenging. Multivariate cryptosystems [13] are explored for both encryption and digital signatures. Some asymmetric key encryption techniques based on multivariate polynomials were shown to be unsafe in a study by Tao et al. because some quadratic connected forms showed poor rank in their central maps. Tao et al. suggested a unique and effective multivariate method dubbed Simple Matrix, which makes use of matrix multiplication, to overcome these problems. Parallel to this, multivariate cryptosystems are essential to digital signatures; two especially useful varieties are Rainbow and Multivariate quadratic equations for Unbalanced Oil and Vinegar (UOV). Larger public key sizes are the outcome of UOV, which is typified by a substantial ratio (3:1) between variables and equations. This causes signatures to be three times longer than the original hash values. Rainbow, on the other hand, works more effectively by using lower ratios, which leads to reduced size of keys and encrypted signatures.

b. Hash Based Signatures:

The Lamport scheme, a type of hash-based signature, was introduced by Leslie Lamport in 1979 and further discussed by Buchmann et al. [17]. One of the parameters, 'b,' determines the intended system's level of safety. HMAC is employed, where a random input value is subjected to a secure hash function that has a hash output length of 256 bits for a security parameter of 128 bits [21]. The recommendation made inside a message is SHA-256.

1. Performance Analysis of Efficient Cryptographic Techniques for CC Security:

Taking into account the need for stability and improved protection of information in the present conditions of the developing world, cryptographic methods are required to guarantee the confidentiality, authenticity, and safety of the transferred data. The application of the cryptographic algorithm that can still withstand the emerging threats, for example, those posed by quantum computing, grows as the computational density rises. Essentially, the focus of this work entails a performance comparison of secure cryptographic algorithms suitable for fortifying the security of CC. They include assessment of aspects that relate to memory usage, computation time, keys sizes, kinds of encryption and overall security perspective and hence offer information on how those methods perform in cloud environment. It is for this reason that the findings that the subsequent research seeks to reveal regarding the effectiveness of some cryptographic techniques as indicated in table 1 will go a long way in ensuring that the right decisions in instances where decisions regarding the design and features of safe and scale cloud-based systems are being made.

Table 1: Evaluation of Effective Cryptographic Methods for CC Security in Terms of Performance

Techniques	**Developed By**	**Key-size**	**Encryption Type**	**Execution time**	**Memory Usage**	**Security Level**
DES	IBM	64 bits	Symmetric	Same as AES	More than AES	Secure for the client & provider
AES	Joan Daemen & Incent Rijmen	128, 196 & 256 bits	Asymmetric	Very fast	Low RAM	Secure for both client & provider
RSA	Rivest-Shamir-Adleman	>1024 bits	Asymmetric	Slowest	Highest memor	Only secure for Client

					y usage	
Blowfish	Bruce Schneier	32-448 bits	Symmetric	Fast	<5kb	Secure for the client & provider
Partial HE	Various (e.g., RSA, ElGamal, Paillier)	smaller	Public-key	Lower	Moderate	Depends on implementation and key size
Somewhat HE	Various (e.g., BGV, BFV, NTRU)	Larger than PHE, but smaller than FHE	Public-key	Higher than PHE, lower than FHE	High	Depends on implementation and parameters
Full HE	Craig Gentry (2009), subsequent improvements	Very large	Public-Key	Higher	Very High	Depends on implementation and parameters, considered theoretically secure
KP-ABC	Sahai and Waters (2005)	Variable, dependent on attribute complexity	Public key	slower than CP-ABE	Can be high for complex policies	Currently considered less secure than CP-ABE
CP-ABC	Bethencourt, Sahai, and Waters (2007)	Variable, dependent on attribute complexity	Public key	Faster than KP-ABE	Can be high for complex policies	Currently considered more secure than KP-ABE
LW ECC	Various researchers	Variable (typically 256-512 bits)	Public Key	Slower than Traditional ECC	Moderate	Post-quantum secure (resistant to quantum attacks)
LW Hash Function	Various researchers	Variable (typically 256-512 bits)	Hash Functions	Fast (similar to SHA-256)	Low	Post-quantum secure (resistant to quantum attacks)

Lattice Based	Various researchers	Generally larger than traditional algorithms (e.g., 1000-5000 bits)	Post Quantum Cryptography	Can be slower than traditional algorithms, but ongoing research is improving efficiency	Can be higher than traditional algorithms, depending on the specific scheme	Post-quantum resistant (believed to be secure against quantum computers)
Multivariate	Various researchers	Typically smaller than lattice-based algorithms (e.g., 128-256 bits)	Post Quantum Cryptography	Can be slower than traditional algorithms, especially for larger key sizes	Can be higher than traditional algorithms, depending on the specific scheme	Resistant to some classical attacks, but some schemes have been broken
Hash based signature	Various researchers	Depends on the hash function used (e.g., 256 bits for SHA-256)	Post Quantum Cryptography	Relatively fast, especially for verification	Low compared to other public-key algorithms	Security depends on the underlying hash function, but can be very strong

5. Discussion and Future work

This survey then presented several significant concerns on the new and efficient cryptographic techniques for cloud computing security explored in this article. Firstly, it was always a contentious issue because of the danger of compromising security in an attempt to increase efficiency, which is also the case here. Albeit the traditional mathematical algorithms like AES and RSA provide maximum security their computational time can be antagonizing when implemented in an environment, specifically cloud platforms. On the other hand, light-weight solutions provide solutions that offer a measure of security at the expense of providing higher response rates. As for promising paradigms, homomorphic encryption initiatives and lattice-based cryptography give a hope for creating a secure cloud data that will still be usable. These techniques enable computation of data without actually decrypting it, a factor that is crucial in abating data corruption in cloud environments. Though in theory they sound effective and efficient, in practice, concerns arise when it comes to computational time and management of keys. There is also another excellent feature of the survey: it is the accent on the interaction of some techniques which is normally used as a part of a set of methods with the best features of each of them being employed to achieve the most effect. For example, the combination of lightweight ciphers with homomorphic encryption may bring optimization in development for a relatively safe level. Moreover, use of multi-party computation also increase the security of data that is being processed since it can be processed in parallel with different parties without exposing any information that is considered confidential. Lastly, owing to an increased utilization of cloud computing, the analysis of advanced technologies such as blockchain and Quantum computing should be further explored and conducted in the future, distributed ledger application of Blockchain can increase the data reliability and efficiency, whereas quantum computation remains a major challenge that can weaken existing Cryptology Algorithms .

Based on the results of the systematic survey, the following directions can be regarded as critical research and development areas in the context of cryptographic methods for cloud computing security. They are these directions that can bring about the possibilities for new developments which override present day drawbacks and post likely future difficulties that may arise.

6. Conclusion

From the recent work reviewed in Section IV it was witnessed how cryptographic techniques for cloud security have evolved and are changing. The results of the survey of the cloud computing challenges therefore underlines the importance of addressing them while raising awareness of the current work that experts and academics in the field are doing to advance the security in the technology. Al a time, such advanced cryptographic algorithms can improve cloud-based systems security. However, it is essential to remain weary and open to other risks which should drive more research and development in this field. This work renders a vision over existing trend in efficient cryptographic algorithms and clears the path for future developments regarding security of cloud computing, thereby recommended to academicians, practitioners as well as policy makers.

References:

[1] Mathur, P. “Cloud Computing Infrastructure, Platforms, and Software for Scientific Research. Series in Bioengineering”. pp-89-127, January 2024, doi.org/10.1007/978-981-97-1017-1_4.

[2] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, “A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing,” International Journal of Intelligent Networks, vol. 3, pp. 16–30, Jan. 2022, doi: 10.1016/j.ijin.2022.04.001.

[3] K. S. Rao and V. H. Shastri, “a review on various cryptography techniques in cloud security,” International journal of advance research in science and engineering. Volume No 6 special issue No (01).

[4] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, “Cloud data security and various cryptographic algorithms,” International Journal of Electrical and Computer Engineering, vol. 13, no. 2, pp. 1867–1879, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.

[5] P. Karthikeyan, “Genetic algorithm with self adaptive immigrants for effective virtual machine placement in cloud environment,” International Journal of Intelligent Networks, vol. 4, pp. 155–161, Jan. 2023, doi: 10.1016/j.ijin.2023.07.001.

[6] F. Thabit, O. Can, R. U. Z. Wani, M. A. Qasem, S. B. Thorat, and H. A. Alkhzaimi, “Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms,” Concurr Comput, vol. 35, no. 21, Sep. 2023, doi: 10.1002/cpe.7691.

[7] F. Thabit, S. Alhomdy, and S. Jagtap, “A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions,” International Journal of Intelligent Networks, vol. 2, pp. 18–33, Jan. 2021, doi: 10.1016/j.ijin.20.03.001.

[8] B. Rahul and K. Kuppusamy, “Efficiency Analysis of Cryptographic Algorithms for Image

Data Security in Cloud Environment," IETE J Res, vol. 69, no. 9, pp. 6053–6064, 2023, doi: 10.1080/03772063.2021.1990141.

[9] H. Sharma, R. Kumar, and M. Gupta, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," in 2023 2nd International Conference for Innovation in Technology, INOCON 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/INOCON57975.2023.10101044.

[10] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based Encryption for Cloud Computing Access Control: A Survey," ACM Computing Surveys, vol. 53, no. 4. Association for Computing Machinery, Sep. 01, 2020. doi: 10.1145/3398036.

[11] Nauman, U., Zhang, Y., Li, Z., & Zhen, T. (2024, March 13). Q-ECS: Quantum-Enhanced Cloud Security with Attribute-based Cryptography and Quantum Key Distribution. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-4006533/v1

[12] G. K. Mahato and S. K. Chakraborty, "A Comparative Review on Homomorphic Encryption for Cloud Security," IETE Journal of Research, vol. 69, no. 8. Taylor and Francis Ltd., pp. 5124–5133, 2023. doi: 10.1080/03772063.2021.1965918.

[13] E. S. Alu., K. Yunana, and M. U. Ogah, "Secured Cloud Data Storage Encryption Using Post-Quantum Cryptography," IJARCCE, vol. 11, no. 7, Jul. 2022, doi: 10.17148/ijarcce.2022.11704.

[14] M. K. Sasubilli and R. Venkateswarlu, "Cloud Computing Security Challenges, Threats and Vulnerabilities," in Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 476–480. doi: 10.1109/ICICT50816.2021.9358709.

[15] U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi, and N. Albaqami, "Cloud Security Threats and Solutions: A Survey," Wireless Personal Communications, vol. 128, no. 1. Springer, pp. 387–413, Jan. 01, 2023. doi: 10.1007/s11277-022-09960-z.

[16] O. Can, F. Thabit, A. O. Aljahdali, S. Al-Homdy, and H. A. Alkhzaimi, "A Comprehensive Literature of Genetics Cryptographic Algorithms for Data Security in Cloud Computing," Cybernetics and Systems. Taylor and Francis Ltd., 2023. doi: 10.1080/01969722.2023.2175117.

[17] K. M. Hussein and M. F. Al-Gailani, "An Efficient Bandwidth Based on the Cryptographic Technique of the RSA Accumulator in Block Chain Networks," in Proceedings - CSCTIT 2022: 5th College of Science International Conference on Recent Trends in Information Technology, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 164–168. doi: 10.1109/CSCTIT56299.2022.10145614.

[18] A. Kousalya and N. kyun Baik, "Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique," International Journal of Intelligent Networks, vol. 4, pp. 62–67, Jan. 2023, doi: 10.1016/j.ijin.2023.03.003.

[19] Avik, S. C., Biswas, S., Ahad, M. A. R., Latif, Z., Alghamdi, A., Abosaq, H., & Bairagi, A. K. (2023, November 26). Challenges in Blockchain as a Solution for IoT Ecosystem Threats and Access Control: A Survey. arXiv.org. https://arxiv.org/abs/2311.15290

[20] M. Kumar, S. Farhat, and M. S. Alam, "light weight security scheme of cloud storage system based on ecc (CURVE25519)," International Journal of Technical Research & Science, vol. Special, no. Issue3, pp. 1–10, Oct. 2020, doi: 10.30780/specialissue-icaccg2020/034.

[21] S. Windarta, S. Suryadi, K. Ramli, B. Pranggono, and T. S. Gunawan, "Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions," IEEE Access, vol. 10, pp. 82272–82294, 2022, doi: 10.1109/ACCESS.2022.3195572.

[22] G. B. Satrya, Y. M. Agus, and A. Ben Mnaouer, "A Comparative Study of Post-Quantum Cryptographic Algorithm Implementations for Secure and Efficient Energy Systems Monitoring," Electronics (Switzerland), vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183824.

[23] K. Sundar, S. Sasikumar, C. Jayakumar, D. Nagarajan, and S. karthick, "Quantum cryptography based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing," Multimed Tools Appl, vol. 82, no. 27, pp. 42817–42832, Nov. 2023, doi: 10.1007/s11042-023-15463-1.

[24] Mushtaq, M. A., Sultan, A., Afrasayab, M., Zubair, T., & Abid-bin-Shakir. (2019). New Cryptographic Algorithm Using ASCII Values and Gray Code (AGC). Proceedings of the 2019 4th International Conference on Big Data and Computing - ICBDC 2019. https://doi.org/10.1145/3335484.3335540