Alkadhim Journal for Computer Science, Vol. 2, No. 1 (2024)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

A Review of Encryption Algorithms for Enhancing Data Security in Cloud Computing

[1,2]Doaa S. Salman[*], [3]Nasri Sulaiman

[1]Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics. Baghdad, Iraq.

[2]Imam Al-Kadhum College. Baghdad, Iraq.

[3]Department of Electrical and Electronic Engineering, Faculty of Engineering Universiti Putra Malaysia;

Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysia. nasri_sulaiman@upm.edu.my.

Article information

Article history:
Received: January, 16, 2024
Accepted: February, 24, 2024
Available online: March, 14, 2024

Keywords:
Cryptography,
Cloud Computing,
Symmetric and Asymmetric Algorithms,
Hybrid Encryption,
Lightweight Algorithms,
Security Requirements.

Corresponding Author:
Doaa S. Salman
doaa.sa.salman@gmail.com

DOI:
https://doi.org/10.53523/ijoirVolxIxIDxx

Abstract

Cloud computing is one of the most rapidly evolving technologies today; it provides numerous advantages that increase its affordability and dependability for use in the company. This paper goes over the concepts of cloud computing, such as its characteristics, deployment model, and service model, discusses the various benefits of cloud computing, and highlights the most pressing issues and security concerns in cloud storage. As a consequence, that leads to a review of distinctive cryptography algorithms that meet the security requirements (CIA: confidentiality, integrity, and availability) that are used to secure communications in cloud computing situations. It also displays many algorithms depending on the previous studies, such as Blowfish, RSA, DES, AES, MD5, Feistel, SP, HIGHT, LED, Cybpher, PRESENT, RC6, Diamond2, mCrypton, SLIM, Klein, PUFFIN-2, SEA, CLEFIA, LBlock, TWINE, 2, ANU, ANU-II, NLBSIT, Piccolo, BORON, RECTANGLE, LICI, QTL, LOGIC, TRIVIUM, Fruit-v2, Fruit-80, A4, the Enocoro family, and Grain family, to make a comparison among them using many measurements. It found that modern and lightweight algorithms are more suitable for use in this field. Furthermore, the purpose of this paper is to make some suggestions for improving the safety and security of cloud computing technologies.

1. Introduction

The cloud is nothing more than a collection of servers and data centers dispersed around the globe and are in charge of offering users on-demand service through the Internet [1]. Cloud computing is widely used for personal, medical, business, and governmental purposes. Much data is stored on the cloud and must be protected from illegal access [2].

One of the foremost pivotal zones of cloud computing is information capacity security. Security becomes a major concern when someone keeps their sensitive data on a platform that is remote and not directly under their control. Data security is required since it puts data at risk both during transmission and storage because anybody with

unauthorized access can view and alter it. A piece of data is secure if it satisfies the following three requirements: availability, confidentiality, and integrity [3].

Cryptography plays a significant role in maintaining the integrity and confidentiality of the data. When hostile people attempt to hack data, they won't be able to obtain helpful information because data has been looked at as encrypted thanks to cryptographic techniques [2]. As a multi-tenant framework, the cloud employments encryption to allow clients more prominent protection and security. Therefore, the option to encrypt cloud storage empowers users to reclaim their personal space. The study of art and science used to create encrypted information and secure data exchange is known as cryptography. Converting plaintext into ciphertext is considered an improved strategy for ensuring data secrecy in cloud systems [4].

Cloud computing, independent of physical location, pools resources and algorithms to supply high-performance administrations [5]. Even though cloud computing rearranges our lives, it also comes with security threats. to protect its clients and help them accomplish their objectives, cloud computing should meet the security requirements of; Confidentiality; It ensures that private information in the cloud is not disclosed by unauthorized users and that it is kept confidential. Privacy; the clients have control over their data in the cloud beyond any doubt, which is stored after being collected by them, or those who authorized them. Integrity; It requires the cloud to guarantee the accurate evaluation of information when (storage, exchange transmission, and recovery) implies that it changes as it were through authorized exchanges and is not manipulated by system users through unauthorized transactions. Availability; ensure that the cloud works immediately and that authorized users are not denied service [6].

There are multiple approaches to protecting cloud infrastructure, such as; using tunneling and including the exploitation of virtual circuits, to ensure communication security. Using distinct servers, storing hashed data, duplication, and server load limit, are all examples of intrusion detection systems (IDSs), to keep the servers safe [7].

Also using signatures in the Internet age, each writer needs a one-time password and verification. Dispersed storing, regional servers, and local disk short-term backup, all that to keep customers safe. To keep the cloud constructed safely, incorporating various characteristics based on the level of protection, and mixing a one-time password as well as a digital signature allowing for two-factor verification. According to analyzed studies, numerous common technologies are employed to mitigate threats to cloud data security, such as; authentication, encryption, data back-ups, and hashing [7].

Encryption is a highly Advocated method to enhance the security of information. It is advisable to encrypt the data before storing it on a cloud server. Encryption, as a fundamental security mechanism, plays a crucial role in safeguarding confidential information in motion and at rest within the cloud infrastructure because codifying data to prevent unauthorized access serves as a valuable measure in safeguarding against data breaches and thwarting unauthorized access [8].

Encryption is the most useful tool for ensuring data protection because it ensures confidentiality, integrity, privacy, and availability in the context of cloud storage security. Organizations must thoroughly evaluate which encryption algorithms and methods align most effectively with their individualized specifications and specifications [9].

In this work, we proposed to grant a survey and in-depth investigation of the encryption and decoding strategies utilized in cloud information capacity to move forward both productivity and security.

2. Problem Statement

There are different outlines of issues and dangers in the technology of cloud computing which incorporate security, storage, isolation, unwavering quality, privacy, and more. But the most imperative among these concerns is security and how to benefit supplier guarantees it to preserve [1]. In the Cloud, a number of security vulnerabilities can occur [10]:

• Ensuring Safe Data Exchange: In the cloud environment, the end- has no dominance on the actual site or reach of the resources that are hosted.

• Ensuring Secure Interface: Over an insecure internet, it is necessary to guaran-tee the benignity of data in transferring, storage, and recovery.

• Data separation: When cloud service providers have access to personal information or when the boundaries between corporate and personal data are not explicitly specified by policies, privacy concerns can arise.

• Secure Stored Data: It's unclear whether the customer or the cloud service provider will be in charge of encrypting and decrypting the data.

• User Access Control: Web data logs for PCI DSS-compliant web-based transactions must be given to compliance auditors and security managers.

Despite its many benefits, cloud computing features plenty of security problems and dangers, including counting assaults, pernicious insiders, information burglary or misfortune, cloning, and extra security challenges attached to virtualization, among others [10].

On June 7, 2022, in both Seattle and the RSA Conference held in San Francis-co, the Cloud Security Alliance (CSA) presented their latest report titled Top Threats to Cloud Computing: The Pandemic 11. As the world's foremost organization committed to defining standards, certifications, and best practices to foster a safe cloud computing environment, the CSA observed a significant shift in the concerns of cloud security providers (CSP) with regard to security issues. This report is the sixth in the Top Threats to Cloud Computing series. Figure (1) appears the security concerns in cloud computing recognized by the CSA. Collectively, the security concerns serve as a summoning to initiate and ameliorate the aware-ness, configuration, and management of cloud security protocols pertaining to identity [11].

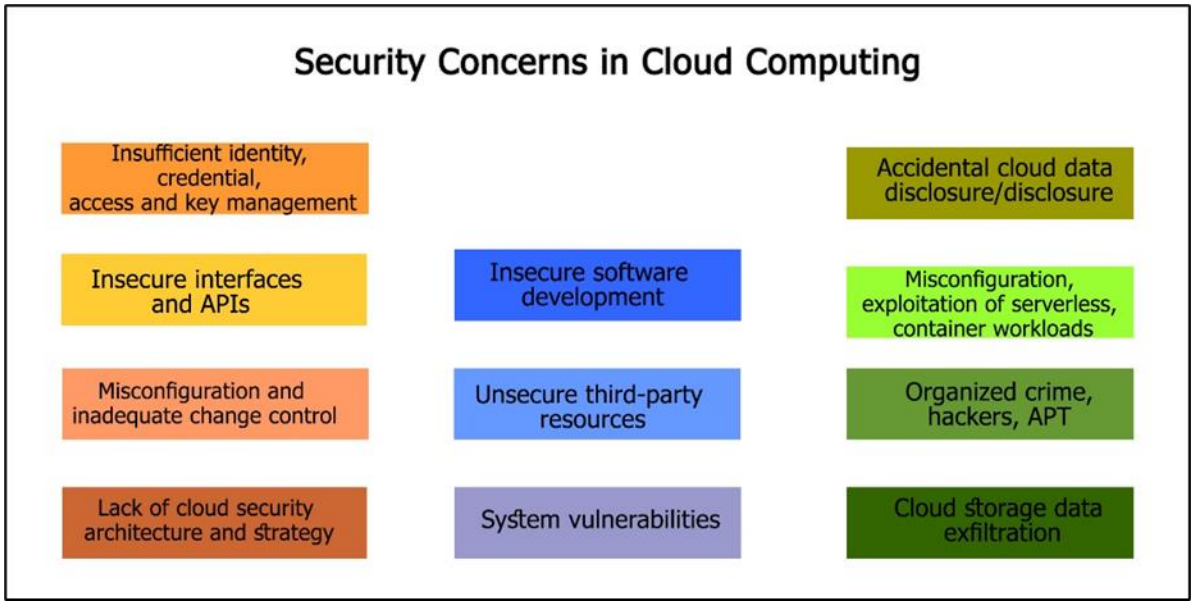

Figure (1): Security Concerns in Cloud Computing Recognized by the CSA.

3. Literature Review

Ahmad et al. (2018) discuss the benefits of cloud service in many dimensions such as; Economic Drivers, Scalability, Resource Utilization, and Ease of Maintenance. In cloud-based data centers, the implementation of automation is deemed essential for expansion. Therefore, it is considered to be a fundamental principle of design. Additionally, the focus on DCN networks centers around the concept of Virtualization, which holds great promise in terms of in-creased performance and maximum reliability. Furthermore, it can be deployed in both server and

storage equipment. However, in comparison to the previously mentioned dimensions, current work is shifting towards the cloud and vast clustered network applications [12].

Abrar et al. (2023) showed the results of common data security threats in cloud computing. The most common threats as; privacy data location, cloud backup, data access controls, authentication, database availability, data integrity, data protection, malicious insider attacks [8].

Oluwasanmi et al. (2023) discuss many studies and according to a study by Ghanam et al (2012), it was observed that security concerns constituted a critical issue in 66 of the assessed research articles. The second-most significant issue was infrastructure, with a score of 46, and data management was the third-most important issue at a score of 15. There are attempts by malicious actors to exploit any new vulnerabilities, data sprawl, application sprawl, and potential cloud infrastructure misconfiguration for their benefit. The impacts of these threats or attacks are diverse, ranging from compromising data integrity or confidentiality to affecting system availability [9].

Hala et al. (2021) discuss the strength of encryption to that whatever operating system you use, whatever programs or authentication mechanisms you implement, the actual strength of the system is highly dependent on encryption and a secret-key steganographic system to withstand attacks against potential methods [13].

Munwar et al. (2022) provides a discussion on two significant issues: the security of stored data and system overload due to the data volume. In plain text storage, the primary challenge is the possibility of data security breaches. Conversely, encrypted text storage may cause system overload due to the encryption of complete file data. To address these concerns, we propose a viable solution in the form of a new service model, Confidentiality-based Classification-as a-Service (C2aaS). This model processes data dynamically and classifies it into confidential and non-confidential categories based on its security level. The data is then encrypted as required before being stored in the cloud. Our proposed service model outperforms conventional methods by providing robust security for confidential data and reducing cloud system overloading [14].

Tristan et al. (2023) the present study aims to provide an all-encompassing overview of the Encryption Key Management Services proffered by two of the most predominantly utilized Cloud Service Providers (CSPs), namely Amazon Web Services (AWS) and Google Cloud Platform (GCP). Both ser-vices have exhibited commendable performance in data encryption and key management. A comprehensive analysis of each Key Management Service was conducted to gain a thorough understanding of their capabilities, use cases, and shortcomings. Based on the results, it can be inferred that AES-256 emerged as the unequivocal winner for symmetric encryption key usage, while RSA proved to be the optimal choice for asymmetric encryption keys [15].

Khasim et al. (2017) primarily focuses on how to assess and analyze the most significant security encryption algorithms for cloud computing data protection. In the present study, a variety of encryption algorithms, namely RSA, AES, DES, and Blowfish, are employed with the aim of guaranteeing data security within the context of cloud computing. The success ratio of the algorithm has been found to be contingent upon two salient factors, namely, the secrecy of the key and its distribution. As demonstrated in this paper's simulation, the encryption algorithms' influence can be observed in the consideration of two crucial parameters, namely, throughput and processing time. When higher throughput is present, the speed increases, and in such instances, power consumption is also observed to be lower. Ultimately, it is deduced that Blowfish is the most optimized algorithm among all available ones. Also, it's preferred for more accurate results it needed to use many measuring metrics to account for throughput as; CPU time, encryption, and decryption, memory usage, and energy consumption, all of which have an impact on the algorithmic qualities [16].

Abid et al. (2019) proposed a security architecture for a cloud computing system. The system comprises an AES file encryption system in conjunction with an Elliptic cryptosystem for secure communication. Additionally, the use of One-time passwords for user authentication and SHA2 as a hashing algorithm ensures data integrity and the authentication of data. As a result, this model guarantees security for the entire cloud computing system. Despite the complexity of the system, the execution time remains reasonable due to the implementation of the algorithm on dispersed servers. In our proposed system, an intruder would find it arduous to gain access to information or

upload files as they would need to take control of all the servers. Thus, the proposed system provides a robust secu-rity framework for cloud computing [17].

Shakeeba et al. (2015) discuss the concept of enhancing the security of Cloud Computing through the utilization of cryptographic algorithms. However, it is important to note that current cryptographic algorithms solely operate at a single level of encryption. This presents a considerable vulnerability to cyber-criminals who can effortlessly breach single-level encryption. To address this issue, the proposition of a system that employs multilevel encryption and decryp-tion has been put forth in order to fortify the security of Cloud Storage. [18].

Mawaddah et al. (2021) to conduct a thorough analysis, it is im-perative to compare encryption algorithms based on three essential metrics: CPU time, encryption time, and decryption time, but the result is not so accurate or different depending on the measured metric, the parties arrived at a consensus that RSA algorithm exhibited lower computational efficiency in comparison to AES and MD5 algorithms. However, the utilization of memory usage as an auxiliary metric demonstrated the superiority of AES over RSA, and when conducting a comparison between AES and Blowfish, it was found that the latter outperformed the former. However, it should be noted that the measuring metrics used in this analysis were limited. As such, it is recommended that additional performance indicators, such as throughput of encryption, throughput of decryption, encryption time, decryption time, CPU process time, CPU clock cycles, power consumption, diffusion analysis, and memory utilization, be employed in order to enhance the efficacy of these algorithms [2].

Ijaz et al. (2020) talk about the algorithm of homomorphic cryptography as one method which has attracted interest, it is used to protect customer data on cloud servers. The specialists who contributed to this article ran algorithms utilizing ciphertext fabric that might be utilized straightforwardly without jeopardizing the security of the encryption procedures. Using a completely homomorphic cryptographic algorithm, a framework has been established by the researchers to ensure safeguarding of data that is stored in the cloud. SDC; Fully Homomorphic Encryption (FHE), Paillier, and RSA are the three homomorphic cryptographic algorithms that were tested for complexity using encryption, decryption, throughput, and memory utilization. They found that FHE is the most effective strategy for safeguarding user data preserved in the cloud because it allows users to execute additive and multiplicative operations on encrypted data without having to decode it on cloud servers [19].

Krishna et al. (2017) offered a structure for Improving the security and the data privacy of the owner in cloud computing. The dual round key characteristic of the modified 128 AES method was used to compare the AES and the proposed Improvement AES utilizing the encryption speed of 1000 blocks per second. Encryption, decryption, the employing of energy, network utilization, network de-laying, trustworthy devices, and as well as service management de-vices are just a few of the several parameters that are compared. Real-time apps employ the same algorithms. Their architecture reduced energy use by 14.43%, utilization of the network by 11.53%, and delay by 15.67%, as stated by the data. Consequently, the indicated framework has been improving the security, re-source usage decreasing, and shortening latency when providing cloud computing services [20].

Zheng et al. (2011) also showed how to combine two distinct algorithms, like DES and RSA, to eliminate the security challenges of cloud storage. Identified and conducted research on previous research on cloud data security. They proposed a hybrid security cryptographic tactic that employments Blowfish and MD5 to improve the security of cloud servers [21].

Princy (2015) discusses the goal of this work was to determine the outcome using several cryptographic algorithms with various orientations and parameters such as; RC4, RC6, DES, DES3, AES, and BLOWFISH. Different symmetric key algorithms' energy consumption was studied, and it was found that whereas AES is speedier than other algorithms, so there's an 8% enhancement in power utilization. The Blowfish algorithm, when compared to other symmetric key algorithms, is deemed to be more secure and also yields optimal results with minimal processing time and fewer rounds [22].

Fursan et al. (2021) proposed a new lightweight cryptographic algorithm, called a New Lightweight Cryptographic Algorithm (NLCA) in the realm of cloud computing, the fortification of data security is of utmost importance. To this end, encryption based on symmetric cryptography is utilized. Specifically, a 16-byte (128-bit) block cipher

algorithm requiring a 16-byte (128-bit) key is employed. The algorithm, inspired by the Feistel and SP architectural methods, greatly enhances encryption complexity and is both simple and highly secure. To appraise its effectiveness, the proposed algorithm is compared to frequently used crypto-graphic algorithms - namely DES, AES, HIGHT, Blowfish, and LED - using various parameters, including block size, key length, possible key, mathematical operations, cipher type, and security power. The experimental results demonstrate that the NLCA algorithm provides powerful security and a marked improvement in encryption/decryption, with high security and low computation cost. Particularly for the fast-paced world of cloud computing, this algorithm is especially effective in relation to data collection and processing time [23].

Noor et al. (2022) proposed a thorough analysis of lightweight and ultra-lightweight encryption algorithms, taking into account both the most recent symmetric key ciphers (Block and Stream) and the most recent cryptanalysis findings. The last two concentrate on strengthening device security with con-strained resources by consuming less memory, computing power, and energy. Due to the extremely low resource and power demands of lightweight algorithms, they operate extraordinarily quickly and can handle little amounts of data. They talk about 18 different types of light block ciphers, including mCrypton, SLIM, Klein, Present, PUFFIN-2, SEA, CLEFIA, LBlock, TWINE, 2, ANU, ANU-II, NLBSIT, Piccolo, BORON, RECTANGLE, LICI, and QTL. Additionally, we'll talk about six other types of light stream ciphers, including LOGIC, TRIVIUM, Fruit-v2 and Fruit-80, A4, the Enocoro family, and The Grain family. As a result, using lightweight cryptographic algorithms is one of the best ways to protect those IoT applications. Currently, one can categorize it as a trend that is anticipated to in-crease throughout the upcoming years as a result of the development of IoT sys-tems [24].

Jack et al. (2023) presented a lightweight algorithm called Cybpher, a new kind of Lightweight Encryption Algorithm (LEA) that aims to become a standard in the world of LE Algorithms. They have also demonstrated with tests how fast it is and computationally easy. Cybpher can also be considered secure against plaintext attacks and brute force attacks when the key is truly random and the Key and Offset Buffers remain well protected [25].

Azni et al. (2023) discusses the intricacies surrounding lightweight encryption algorithms in mHealth systems with a view to conducting a comparative analysis vis-à-vis data privacy in the wireless perception layer, such as; AES, PRESENT, HIGHT, CLEFIA, CAMELLIA, TWINE, SPECK, SIMON, RECTAN-GLE, SPARX. The findings of the analysis indicate that RECTANGLE may offer superior efficiency in comparison to alternative options. Furthermore, an enhanced version of RECTANGLE in 3D has been suggested to fulfill the aforementioned criteria, which provides better protection for its rotation in contrast to 2D RECTANGLE. As a result, the number of rounds can be reduced for the proposed algorithm, which guarantees increased security for the rotation of every plaintext value. This results in a secured mHealth algorithm for future use [26].

Noor et al. (2022) proposes a novel approach to chaotic keys generation, based on 4-D NSJR chaotic systems. The suggested system exhibits a remarkable capability of generating a significant number of key sequences. It encompasses four distinct phases, namely the input, key generation, encryption, and output phases. During the key generation phase, the novel 4-D NSJR chaotic system was employed. Moreover, the system recommends the inclusion of the P-Layer from the PRESENT Block Cipher with the Diamond2 lightweight Block Cipher, with the aim of achieving the utmost protection level, alongside enhancing the encryption/decryption speed and fortifying it against established cryptanalysis attacks. The proposed system passed the NIST test suit, and numerous measurements were conducted [27].

Samar et al. (2022) this paper aims to provide a comprehensive over-view of the fundamental concepts of cryptography, with a specific focus on the theoretical background of symmetric ciphers. The two main types of symmetric ciphers, namely stream and block ciphers, will be discussed in detail. Additionally, the main concepts of the components used in symmetric ciphers will be presented. Finally, a selection of modern and lightweight symmetric algorithms will be examined. The present review endeavors to present the cipher algorithm based on the fundamental components that are utilized in cipher design. This paper seeks to explain how these components, including kind, numbers, and sizes, im-pact the classification of the cipher algorithm and its performance, area, and weight. It provides RC4, Salsa20, A5/1, Des, AES, Blowfish, and IDEA as Modern algorithms. Also provide LOGIC, A4, DESL, LBlock, TWINE, Simon, Speck, RECTANGLE, QTL, BORON, NLBSIT, and SAND-64 as lightweight algorithms. and Fruit-v2 as Ultra-lightweight [28].

4. Cloud Computing Concept

A cloud is a collection of servers and datacenters that are dispersed through-out the world and are in charge of offering users on-demand service through the internet [1]. By hosting their apps on the cloud, different firms can make it easier for people to use remote information technology (it) resources, which is considered a trend. The cloud service is not available on the user's machine. These services must be subscribed to in order for the user to access them online. The fundamental benefit of cloud computing is that it removes the requirement for users to physically be present in the same place as the gear, software, and storage space. Without worrying about maintaining gear, software, and storage space, you may save and retrieve your data using the cloud from any location at any time. Users can access all of these services at a reasonable price. According to the amount of storage space the user uses, he must pay. Everyone is moving their data to the cloud because of this flexibility [2].

4.1 Cloud Essential Characteristics

Cloud computing offers low-cost Internet-based services for resource sharing. A model for empowering all inclusive, on-demand network, it is advantageous to have access to a shared pool of adaptable computational resources, encompassing servers, storage, networks, applications, and services, that can be rapidly purvey and discharged with minimal administration or service provider potential, that is done by (NIST) is an acronym for the National Institute of Standards and Technology, a U.S. government organization, defines as cloud computing [29]. The NIST decides a cloud basic characteristic as taking after [2]:

- On-demand self-service: Through an internet control board, clients can naturally get to cloud administrations and assets as required without reaching the benefit supplier.

- Broad access: Cloud computing offers the network's accessible capabilities through an assortment of the various stages of clients, such as phones, tablets, laptops, and portable workstations.

- Resource pooling: The computing belongings (applications, capacity, preparing, and organizing transfer speed) of the administration's supplier are combined as fundamental to suit different shoppers.

- Measurable service and management: By checking, overseeing, detailing, and encouraging straightforwardness for both the benefits supplier and the client of the utilized benefit, cloud frameworks give mechanized control and proficient asset utilization.

- Quick and elastic services: Cloud computing offers versatile and versatile administrations to meet the desires of clients. Programs, assets, clients, and any other highlights can be included or removed without causing a struggle within the cloud.

4.2 Cloud Computing Deployment Models

The NIST distinguished four strategies for sending the cloud demonstration (private, public, community cloud, and hybrid). In the term “public” cloud computing, the framework is made accessible to the common open and is controlled by a cloud supplier who is additionally in charge of overseeing and running the cloud's inner operations. Oppositely, in a "private" cloud, the foundation is as it was utilized by a single commerce and is kept up by that organization straightforwardly or by a third party; the Cloud Supplier (CP) is exclusively in charge of the infrastructure [2].

By providing framework of public and private clouds which are two illustrations of the two or more sorts of clouds that make up "hybrid" cloud computing design [2]. The final form of cloud is "community" cloud; in this sort, a few businesses who share a few of similar concerns, such as duty, security prerequisites, approach, etc., share the cloud framework. The organizations or another third par-ty may be in charge of overseeing the foundation of this sort [6].

4.3 Cloud Computing Services Models

The cloud administrations can be given to clients in three distinctive benefit models [30] or this model called the SPI model encompasses the constituent components of each layer along with the associated administrative obligations of both the provider and the customer:

- Software as a Service (SaaS): This model gives users online web browser or application interface gets to various computer program applications and assets kept in a far-off location.

- Platform as a Service (PaaS): This gives clients all the instruments they ought to make and send applications within the cloud utilizing any programming dialects, libraries, devices, or administrations that the suppliers give. In this worldview, the buyer can as it were overseeing the conveyed apps and environment parameters for the application-hosting environment and has no administration or control over the cloud foundation.

- Infrastructure as a Service (IaaS): This service type gives customers access to infrastructure resources like hardware, data storage, network resources.

4.4 Cloud Computing Security Issues

All enterprises encounter security hazards, perils, and obstacles on a daily basis. A common misconception is that these words are interchangeable, however, they possess intricate nuances. Discerning the subtle disparities amid them will facili-tate the enhancement of safeguarding your cloud possessions. A "Risk" denotes a likelihood of losing data or a vulnerability. A "threat" embodies a form of assault or adversary. A "challenge" alludes to the impediments organizations face when implementing practical cloud security.

In Figure (2) addresses cloud security issues for all three aspects with the previous concerns of CSA, to ensure the foundation remains free from any form of structural deformity, it is imperative that no cracks exist. The various lenses or angles through which cloud security can be viewed must be taken into consideration. A comprehensive strategy is necessary in order to manage risk (via the implementation of security controls), counteract threats (by means of secure coding and deployment), and surmount obstacles (through the utilization of both cultural and technical solutions), thereby enabling businesses to securely grow through the use of cloud technology [31].

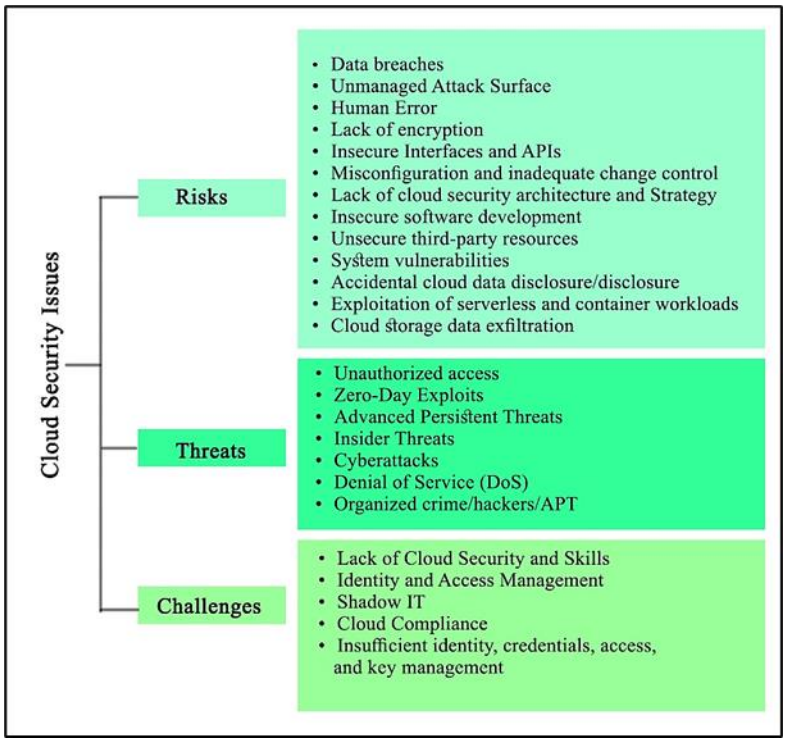

Figure (2): Cloud Security Issues.

4.5 Cloud Service Provider

A Cloud Service Provider (CSP) is an organization that provides certain cloud computing elements, as per academic conventions, which is the term for the on-request, as soon as the dissemination of IT services via the Internet occurs, payment shall be rendered. The option to procure technological services, which include storage, processing power, and databases, rather than the procurement, operation, and maintenance of data centers and physical servers, is made available, as well as platform-specific certifications that demonstrate experience in a given cloud provider [32]. The preeminent public cloud service providers encompass Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure [15] on an as-needed, cloud services may be acquired from a provider such as:

4.5.1 Amazon Web Services (AWS)

A web service named AWS Identity and Access Management (IAM) is used to manage to get access the services of AWS as securely. IAM enables centralized administration of user accounts and security credentials, including access keys, and also demonstrates how to apply access control policies to secure your re-sources. Additionally demonstrates how to establish a connection with other identity services to allow visitors to access your AWS resources [33].

4.5.2 Microsoft Azure platform

Azure is a platform for public cloud services that supports a wide range of devices, operating systems, programming languages, frameworks, and tools. It's capable of functioning with Linux containers whilst also integrating with Docker. It has the ability to execute programs written in Python, PHP, Java, JavaScript, NET, and Node.js, in addition to creating back-end solutions for Android, iOS, and Windows devices. The infrastructure of Azure has been constructed for hosting millions of clients concurrently, from the building to the apps, and it offers a solid platform on which companies may come upon their security needs. The Azure Security Engineer associate attests to your proficiency in setting up security services and data protection [34].

Microsoft Defender for Cloud is an application that manages your environment's overall security posture in the cloud, protects your workloads in multi-cloud and hybrid environments against changing threats, and identifies security gaps throughout your cloud configuration [35].

4.5.3 Google Cloud Platform

The third and last provider, Google Security Engineer, rounds off the top three and demonstrates your proficiency with Google cloud architecture and implementation. The fundamental components are comparable to Azure and AWS, and knowledge of topics like identity and access control, data protection, and key management is required. Using the industry's premier data cloud, make better decisions. Running and developing your apps anywhere. Transform the way your teams work together, use cutting-edge security tools to protect what matters, etc. Dismantle the cells between your explanatory data stores and operational actions to make inventive user practices, gain a global vision of knowledge, utilize data to turn out choices in real-time, and connect with everybody in your organization, may execute and create your programs anywhere else [36].

5. Cryptography Algorithms

The field of cryptography holds a significant position in the integrity and confidentiality of data. The term "cryptography" is determined from the Greek words "cryptos" (mystery) and "graphein" (composing) [37]. It is the ponder of the craftsmanship and science of planning secure and safe information communication; it is fundamental when basic and private information must be secured [38]. Cryptography is a discipline that deals with the method of concealing messages by means of a secret code. Encryption, on the other hand, refers to the process of transforming and decrypting data. The first pertains to the study of techniques used to maintain confidentiality between two parties, such as symmetric and asymmetric keys, while the second is focused on the actual process of encoding and decoding. Meanwhile, cryptanalysis is a scientific field that involves deciphering data and revealing the message in plain text [39].

5.1 Cryptography Algorithms Types

Usually, cryptographic systems rely on three dimensions; symmetric vs. asymmetric encryption, blocks vs. streams, and substitution vs. transposition, to provide different approaches and techniques for achieving specific goals and addressing different security requirements [1]:

1. Symmetric vs. Asymmetric Encryption:

- Symmetric encryption employs an identical key for both the encryption and decryption processes. This methodology boasts high efficiency and is a suitable option for the encryption of extensive data. Nevertheless, it necessitates a secure channel for key distribution, as both parties must have access to the shared secret key.

- Asymmetric encryption employs a pair of keys: the utilization of a public key for encryption, coupled with a private key for decryption, obviates the necessity for a secure key exchange, since the public key may be disseminated without constraint. Asymmetric encryption enables digital signatures, key exchange, and secure communication. However, it is slower and computationally more expensive than symmetric encryption.

2. Blocks vs. Streams:

- Block ciphers process data in fixed-size blocks, typically in chunks of a fixed number of bits. They provide a higher level of security and are suitable for bulk data encryption. Each block is encrypted or decrypted independently using a symmetric key.

- Stream ciphers operate by encrypting data on a per-bit or per-byte basis, typically within a continuous stream. Such ciphers are frequently favored for their speed and appropriateness in real-time communication, wireless networks, and situations where data is transmitted seamlessly.

3. Substitution vs. Transposition Ciphers:

- Substitution ciphers replace elements in the plaintext with corresponding elements in the ciphertext based on predetermined substitution rules or algorithms. They change the identity of symbols.

- Transposition ciphers manipulation of plaintext by modifying the order of characters or blocks thereof, while retaining the original character set. They change the sequence of symbols.

By considering these dimensions, cryptographers and security practitioners can select the appropriate cryptographic techniques depended on the specific demands and constraints of the application or scenario at hand. Table 1, summarizes the differences between common cryptographic algorithm types depending on These techniques and a variety of more robust methods, key numbers, hash functions, and digital signatures [2].

Table (1): Summarizing the Differences Between Common Cryptographic Algorithm Types [1-2].

Algorithm Type	Symmetric Encryption	Asymmetric Encryption	Hash Function	Signature Algorithms
Key Management	Shared Secret key	Public-Private key pair	N/A (no keys)	Public-Private key pair
Key Length	Short	long	N/A (no keys)	long
Speed	Fast	Slower	Fast	Slower
Performance	Efficient	Less efficient	Fast	Less efficient
Applications	Bulk data encryption, symmetric key exchange	Digital signatures, secure communication	Data integrity verification, password storage	Digital signatures, authentication
Examples	AES, DES, 3DES, RC6, chacha20, Present, Speck, Hummingbird.	RSA, ECC.	MD5, SHA-256	RSA, DSA, ECDSA

5.2 Encryption

Encryption is the process of converting data into a coded language to prevent unauthorized access. Encryption is a critical security measure that can protect sensitive data in transit and at rest in the cloud. Encrypting data before it is transmitted to the cloud can help prevent unauthorized access and protect against data breaches. It works by converting data into a coded language using a mathematical algorithm, making it unreadable to anyone who does not have the encryption key [9]. Encryption is considered one of the best solutions for cloud storage security due to several key reasons [41] [42].

- Data Confidentiality: Encryption ensures that the data stored in the cloud remains confidential and inaccessible to unauthorized users. By encrypting the data before it is uploaded to the cloud, even if someone gains unauthorized access to the stored data, they would not be able to decipher the encrypted information without the encryption key.

- Mitigating Data Breaches: In the event of a data breach or unauthorized access, encrypted data provides an additional layer of protection. Even if an attacker manages to bypass other security measures and gain access to the encrypted data, they would need the encryption key to decrypt and make sense of the information. This significantly reduces the impact of a potential data breach.

- End-to-End Security: Encryption can be implemented in a way that provides end-to-end security, meaning the data is encrypted on the user's device be-fore being transmitted to the cloud storage provider. This ensures that the da-ta remains encrypted during transit and storage, minimizing the risk of interception or unauthorized access at any point in the data lifecycle.

- Compliance and Legal Requirements: Many industries and jurisdictions have strict regulations regarding data protection and privacy. Encryption can help organizations meet these requirements by ensuring that sensitive information is appropriately safeguarded. Compliance with regulations such as the General Data Protection Regulation (GDPR) may necessitate the use of encryption to protect personal data.

- Trust in Cloud Service Providers: Encryption allows users to maintain control over their data, even when stored in the cloud. By encrypting data before uploading it, users can trust that their information remains secure, even if the cloud service provider experiences a security breach or has access to the stored data.

- Data Sharing and Collaboration: Encryption can facilitate secure data sharing and collaboration in the cloud. By encrypting files or folders, users can securely share them with specific individuals or groups while ensuring that only authorized parties with the decryption key can access the data.

5.3 Lightweight Encryption Algorithms

Lightweight Encryption (LE) is an emerging type of encryption based on high-speed and lower-power computation. LE is mainly used in IoT and other environments where mini-processors are required to process and transmit information, and for low-power and constrained devices [25].

The weight of an algorithm is determined by the weight of a primitive, which is approximately equal to the amount of time and space resources required for its execution. This weight can be assessed in two distinct states, namely software and hardware. The term lightweightness differs between these states, but it is imperative to consider power consumption. In software, the time complexity of a primitive refers to two concepts, namely the algorithm's speed, which is gauged by the number of clock cycles required to process one byte of data, and the latency. On the other hand, space complexity is mainly concerned with memory (RAM) and the space necessary to store the algorithm [24].

By lowering the number and size of these components and making it clearer how these components contribute to the strength of symmetric ciphers as op-posed to asymmetric ciphers, the modern cipher has been transformed into a lightweight cipher. And based on the previous studies, can divide the following table to compare the algorithms as modern, lightweight, and ultra-lightweight algorithms [28].

From the previous studies we mentioned at [21], [23], [24], [25], [27] the following table to compare algorithms in many criteria as; Cipher classification (Mod-ern or Lightweight or ultra-lightweight algorithms), stream or block cipher, block size, key size, round numbers, and cipher structure.

Table (2): Comparison of Algorithms Based on Many Criteria [21], [31-33], [27].

Algorithms	Cipher Classification	Stream/ Block Cipher	Block Size	Key Size	Round Numbers	Cipher Structure
Blowfish [23]	Modern	Block	64 bits	32-448 bits	16	Feistel
RSA [23]	Modern	Block	Variable	Variable	Variable	Not Work
DES [23]	Modern	Block	64 bits	56 bits	16	Feistel
AES [23]	Modern	Block	128 bits	128, 192, 256 bits	10, 12, 14	substitution permutation network (SPN)
IDEA [24]	Modern	Block	64 bits	128 bits	8	Mix
MD5 [24]	Modern	Stream	Not Work	Variable	Not Work	Hash Function
HIGHT [24]	Ultra-Lightweight	Block	64 bits	128 bits	32	(SPN)

LED [24]	Lightweight	Block	64 bits	64-128 bits	48	(SPN)
Cybpher [27]	Lightweight	Block	64 bits	128 bits	64	(SPN)
PRESENT [25]	Lightweight	Block	64 bits	80, 128 bits	31	(SPN)
RC4 [23]	Modern	Stream	Not Work	Variable	Not Work	Not Work
RC6 [23]	Modern	Block	128 bits	128, 192, 256 bits	Variable	(SPN)
mCrypton [25]	Lightweight	Block	64 bits	64, 96, 80, 128 bits	12 or 24	(SPN)
SLIM [25]	Lightweight	Block	32 bits	80-128 bits	32	Feistel
Klein [21]	Lightweight	Block	64 bits	64-96 bits	12, 16	(SPN)
PUFFIN-2 [24]	Lightweight	Block	64 bits	80, 128 bits	32	(SPN)
SEA [25]	Lightweight	Block	128 bits (Variable)	128 bits (Variable)	16 (Variable)	Feistel
CLEFIA [25]	Lightweight	Block	128 bits	128, 192, 256 bits	18 (Variable)	Generaized Feistel Network (GFN)
LBlock [25]	Lightweight	Block	64 bits	80 bits	32	Feistel
TWINE [25]	Lightweight	Block	64 bits	80,128 bits	36	(GFN)
µ2 [25]	Lightweight	Block	64 bits	80 bits	16	(SPN)
ANU [25]	Lightweight	Block	64 bits	128 bits	25	Feistel
ANU-II [25]	Lightweight	Block	64 bits	80, 128 bits	25	Feistel
NLBSIT [25]	Lightweight	Block	64 bits	64, 80 bits	16	Feistel, (SPN)
Piccolo [25]	Lightweight	Block	64 bits	80, 128 bits	24, 32	(GFN)
BORON [25]	Lightweight	Block	64 bits	80, 128 bits	25	(SPN)
Rectangle [25]	Lightweight	Block	64 bits	80, 128 bits	25	(SPN)
LICI [33	Lightweight	Block	64 bits	128 bits	31	Feistel
QTL [25]	Lightweight	Block	64 bits	64, 128 bits	16, 20	(GFN)
LOGIC [25]	Lightweight	Stream	Not Work	80 bits	Not Work	(SPN)
TRIVIUM [25]	Lightweight	Stream	Not Work	80 bits	Not Work	(LFSR)
Fruit-v2 [25]	Lightweight	Stream	Not Work	80, 128 bits	Not Work	Stream Cipher
Fruit-80 [25]	Lightweight	Stream	Not Work	80 bits	Not Work	Stream Cipher
A4 [25]	Lightweight	Stream	Not Work	80 bits	Not Work	Stream Cipher
Enocoro family [25]	Lightweight	Stream	Not Work	80, 128 bits	Not Work	(PRNG)
Grain family [25]	Lightweight	Stream	Not Work	128 bit	Not Work	Stream Cipher

6. Key Generation System

Keys that are utilized as inputs in the encryption process or decryption process when the length of the Key estimate long, it gets to be more troublesome to decode the cipher content, making the algorithms more efficient and effective [43]. Figure (3) showed the typical encryption key lifecycle likely includes key phases as following:

1. Generation

2. Registration

3. Storage
4. Distribution And Installation
5. Rotation
6. Backup
7. Recovery
8. Revocation
9. Suspension
10. Destruction

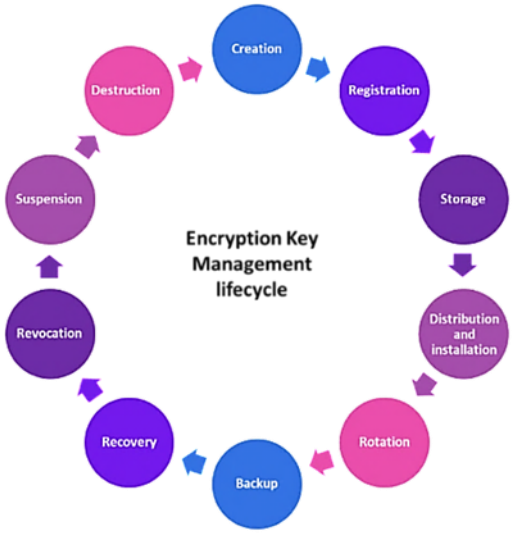

Figure (3): Encryption Key Lifecycle [43].

7. Conclusions

Cloud computing has proven to be a very prosperous application for business-es. Due to the substantial amount of data that organizations need to retain, the utilization of cloud technology provides users with the capacity to store their data while also enabling them to access it from any location at any given moment, private and public corporate organizations and enterprises either have to utilize or plan to use cloud services but are concerned about security, privacy, and data theft. This necessitates the use of cloud security to overcome the cloud environment's acceptance barrier.

For many solutions to support cloud security, we find that cryptography can meet the following goals to ensure cloud security; Confidentiality, Integrity, Authentication, Access Control, Non- repudiation, and Availability.

Therefore, this paper looks at various cryptography solutions that can give high-performance, productive, secured cloud computing, with the advancement of advanced security staying as one of the foremost squeezing issues in the cloud computing world.

All of the research that has been reviewed is founded upon a limited set of two or three cryptographic algorithms that are employed to gauge various metrics, the foremost imperative of which is an encryption/decryption time; in any case, these measurements are inadequate to decide the algorithm's performance. So based on these considers [2] we proposed to examine the algorithms utilizing more execution indicators such as:

- the time of encryption,
- the time of decryption,
- encryption throughput,
- decryption throughput,
- the analysis of diffusion,
- process time of CPU,
- clock cycles of CPU,
- energy consumption,
- Improve the performance of these algorithms using memory utilization.

Based on the comes about of the saw papers, we suggest comparing two se-cured frameworks comprised of two algorithms of hybrid Encryption/decryption to provide a higher level of security. And as the cloud environment is constrained for that it needs low power and fast processing algorithms, which lead us to give a comparison between forty algorithms. To determine the best lightweight algorithms suitable for the cloud environment from the Table 2. I considered the following criteria:

1. Block Size: Cloud environments often deal with large amounts of data, so algo-rithms with smaller block sizes may not be as efficient. I focused on algorithms with larger block sizes to handle data in larger chunks efficiently.

2. Key Size: Algorithms with smaller key sizes may have limitations in terms of security. I looked for algorithms with key sizes that provide a balance between security and computational efficiency.

3. Cipher Classification: I specifically looked for algorithms classified as light-weight in the table, as they are designed to be efficient and resource-friendly in constrained environments like the cloud.

4. Computational Efficiency: While the table does not provide direct performance metrics, lightweight algorithms are generally designed to prioritize computational efficiency and low resource consumption. Algorithms specifically tailored for lightweight implementations were considered more suitable for the cloud environment.

Based on these considerations, I identified the top three lightweight algorithms from the table that are suitable for the cloud environment as PRESENT, LBlock, and TWINE, HIGH, and RC6. These algorithms are designed to provide efficient encryption while minimizing resource consumption and are well-suited for cloud-based applications that operate under resource constraints.

Acknowledgement: This is an optional section.

Conflict of Interest: The authors declare that there are no conflicts of interest associated with this research project. We have no financial or personal relationships that could potentially bias our work or influence the interpretation of the results.

References

[1] T. Ramaporkalai, “Security Algorithms in Cloud Computing,” International Journal of Computer Science Trends and Technology (IJCST), vol. 5, Volume 5 Issue 2, Mar – Apr 2017, [Online]. Available: www.ijcstjournal.org

[2] M. Fouad Alharbi, F. Aldosari, B. Soh, and N. Fouad Alharbi, “Review of Some Cryptographic Algorithms In Cloud Computing,” IJCSNS International Journal of Computer Science and Network Security, vol. 21, no. 9, p. 41, 2021, doi: 10.22937/IJCSNS.2021.21.9.5.

[3] A. Huth and J. Cebula, “The Basics of Cloud Computing,” US-CERT, 2011. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/USCERT-CloudComputingHuthCebula.pdf

[4] S. Jagirdar, J. Srinivas, K. Venkata, S. Reddy, and A. M. Qyser, “CLOUD COMPUTING BASICS,” *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 1, Issue 5, July 2012. [Online]. Available: www.ijarcce.com

[5] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” Computers and Electrical Engineering, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[6] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2020, ISBN-13: 9780135764213.

[7] D.-A. Kumar Pandey Ram Manohar, “A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing AN ANALYSIS OF DATA SECURITY AND PRIVACY IN CLOUD COMPUTING View project Survey of the State of Art of QoS Modeling Approaches View project Ijdiic Ijdiic”, doi: 10.5281/zenodo.7464700.

[8] E. Altulaihan, A. Alismail, E. Altulihan, R. Bukhowah, and M. Frikha, “SECURITY THREATS, COUNTERMEASURES AND DATA ENCRYPTION TECNHINQUIES ON THE CLOUD COMPUTING ENVIROMENT,” J Theor Appl Inf Technol, vol. 15, no. 5, 2023, [Online]. Available: https://www.researchgate.net/publication/369336958

[9] O. R. Arogundade, “Addressing Cloud Computing Security and Visibility Issues,” IARJSET, vol. 10, no. 3, Mar. 2023, doi: 10.17148/IARJSET.2023.10321.

[10] S. Mukherjee, “Cloud-Based Security Solutions,” 2019. DOI: 10.6084/m9.figshare.8312708.

[11] Cloud Security Alliance, July 06, 2022, "Top Threats to Cloud Computing: Pandemic 11 Report". [Online]. Available: https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/.[Accessed: Jun. 05, 2023].

[12] A. N. Quttoum, “Interconnection structures, management and routing challenges in cloud-service data center networks: A survey,” International Journal of Interactive Mobile Technologies, vol. 12, no. 1, pp. 36–60, 2018, doi: 10.3991/ijim.v12i1.7573.

[13] H. A. Naman, N. A. Hussien, M. L. Al-dabag, and H. T. S. AlRikabi, “Encryption System for Hiding Information Based on Internet of Things,” International Journal of Interactive Mobile Technologies, vol. 15, no. 2, pp. 172–183, 2021, doi: 10.3991/ijim.v15i02.19869.

[14] M. Ali, L. Tang Jung, A. Hassan Sodhro, A. Ali Laghari, S. Birahim Belhaouari, and Z. Gillani, “A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security,” Alexandria Engineering Journal, vol. 64, pp. 749–760, Feb. 2023, doi: 10.1016/j.aej.2022.10.056.

[15] A. B. Mailewa, T. L. Moore, S. S. Conlon, A. U. Hewarathna, T. B. M. Dissanayaka, and A. B. Mailewa, "Encryption Methods and Key Management Services for Secure Cloud Computing: A Review." [Online]. Available: https://www.researchgate.net/publication/369777264.

[16] K. Shaik, A. Professor, N. Sharath Kumar, T. Venkat, and N. Rao, "Implementation of Encryption Algorithm for Data Security in Cloud Computing," International Journal of Advanced Research in Computer Science, vol. 8, no. 3, 2017, [Online]. Available: www.ijarcs.info.

[17] A. Hussain, C. Xu, and M. Ali, "Security of Cloud Storage System Using Various Cryptographic Techniques," IOSR Journal of Mathematics, vol. 15, pp. 62–68, doi: 10.9790/5728-1505016268.

[18] S. S. Khan and Prof. R. R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms," International Journal of Innovative Research in Computer and Communication Engineering, vol. 03, no. 01, pp. 148–154, Feb. 2015, doi: 10.15680/ijircce.2015.0301035.

[19] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing," Security and Communication Networks, vol. 2020, 2020, doi: 10.1155/2020/8863345.

[20] K. K. Chennam, L. Muddana, and R. K. Aluvalu, "Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud," in RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 2030–2033. doi: 10.1109/RTEICT.2017.8256955.

[21] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A new family of lightweight block ciphers," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012, pp. 1–18. doi: 10.1007/978-3-642-25286-0_1.

[22] P. Princy, "A Comparison of Symmetric Key Algorithms DES, AES, Blowfish, RC4, RC6: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET), vol. 6, no. 05, May 2015, ISSN: 2229-3345.

[23] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Global Transitions Proceedings, vol. 2, no. 1, pp. 91–99, Jun. 2021, doi: 10.1016/j.gltp.2021.01.013.

[24] J. Rokan, N. Maher Naser, and J. Rokan Naif, "A systematic review of ultra-lightweight encryption algorithms," Int. J. Nonlinear Anal. Appl, vol. 13, pp. 2008–6822, 2022, doi: 10.22075/ijnaa.2022.6167.

[25] J. Wolosevicz, M. Bertaccini "An Introduction to a New Lightweight Encryption Algorithm: Cybpher" Jack Wolosevicz's Lab, March 2023.

[26] A. Halim, "Issues in Lightweight Encryption Algorithm For mHealth A formulation of intelligent algorithm for real time and calculation simplicity for Human Security System based on genetic algorithm approach. View project." [Online]. Available: https://www.researchgate.net/publication/367295749

[27] J. Rokan, and N. M. Naser, “NEW ULTRA-LIGHTWEIGHT IoT ENCRYPTION ALGORITHM USING NOVEL CHAOTIC SYSTEM," *International Journal on ‘Technical and Physical Problems of Engineering* (*IJTPE*), Issue, vol. 53, pp. 253–259, 2022, [Online]. Available: www.iotpe.com.

[28] S. A. Qassir, M. T. Gaata, and A. T. Sadiq, “Modern and Lightweight Component-based Symmetric Cipher Algorithms,” ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY, vol. 10, no. 2, pp. 152–168, Dec. 2022, doi: 10.14500/aro.11007.

[29] P. Mell and T. Grance, “The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology” Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD, 20899-8930. 2011.

[30] B. Gastermann, M. Stopper, A. Kossik, and B. Katalinic, “Secure implementation of an on-premises cloud storage service for small and medium-sized enterprises,” in Procedia Engineering, Elsevier Ltd, 2015, pp. 574–583. doi: 10.1016/j.proeng.2015.01.407.

[31] D. Puzas, Jan. 26, 2023 "CLOUD SECURITY ISSUES: RISKS, THREATS, AND CHALLENGES". [Online]. Available: https://www.crowdstrike.com. [Accessed: Jun. 05, 2023].

[32] W. Chai, "Cloud Service Provider". [Online]. Available: https://www.techtarget.com/searchitchannel/definition/cloud-service-provider-cloud-provider. [Accessed: Jun. 05, 2023].

[33] Amazon Web Services, 2023 "AWS Documentation". [Online]. Available: https://docs.aws.amazon.com. [Accessed: Jun. 05, 2023].

[34] Microsoft Azure, 2023, "Introduction to Azure security". [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/overview. [Accessed: Jun. 05, 2023].

[35] Microsoft Azure, 2023, "Microsoft Defender for Cloud". [Online]. Available: https://azure.microsoft.com/en-us/products/defender-for-cloud/#overview. [Accessed: Jun. 05, 2023].

[36] Google Cloud, 2023, "Why Google Cloud". [Online]. Available: https://cloud.google.com/why-google-cloud/. [Accessed: Jun. 05, 2023].

[37] R. Verma, “SIMULATION-BASED COMPARATIVE ANALYSIS OF SYMMETRIC ALGORITHMS,” International Journal of Advanced Research in Computer Science, vol. 11, no. 5, pp. 64–69, Oct. 2020, doi: 10.26483/ijarcs.v11i5.6655.

[38] Anitha Y, “Security Issues in Cloud Computing-A Review.” International Journal of Thesis Projects and Dissertation (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013, [Online]. Available: www.researchpublish.com

[39] “A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY),” thalesgroup, May 25, 2023. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption (accessed Jun. 05, 2023).

[40] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, “Security Algorithms for Cloud Computing,” in Procedia Computer Science, Elsevier B.V., 2016, pp. 535–542. doi: 10.1016/j.procs.2016.05.215.

[41] K. A. Scarfone, M. P. Souppaya, and M. Sexton, “Guide to storage encryption technologies for end user devices,” Gaithersburg, MD, 2007. doi: 10.6028/NIST.SP.800-111.

[42] E. Barker, “Recommendation for key management: part 1,” NIST SP 800-57 Part 1 Rev. 5, Gaithersburg, MD, May 2020. doi: 10.6028/NIST.SP.800-57pt1r5.

[43] “What is the Encryption Key Management Lifecycle?,” webpage: thales group, May 25, 2023. https://cpl.thalesgroup.com/faq/key-secrets-management/what-encryption-key-management-lifecycle (accessed Jun. 05, 2023).