A Detailed Analysis of Secure and Efficient Data Storage Techniques in Cloud Computing

Syed. Shanawaz Basha, N. Musrat Sultana

Programmer, Chaitanya Bharathi Institute of Technology (A), Hyderabad

Assistant Professor, CSE-Dept, Mahatma Gandhi Institute of Technology (A), Hyderabad

Abstract: *Cloud services have transformed how businesses and individuals store, access, and manage data and applications, owing to their efficiency, reliability, and cost-effectiveness. Both businesses and individuals widely adopt cloud services for these reasons. The proliferation of cloud services has necessitated the implementation of robust security measures to address user concerns. Secure cloud computing ensures that users can access data and services securely, necessitating new strategies compared to traditional models, with cryptographic technology playing a central role. Machine learning (ML)-based approaches have emerged as valuable tools to enhance cloud infrastructure security, particularly when combined with real-time data processing and threat intelligence. This article focuses on various security measures implemented in cloud data storage and security, highlighting ML techniques and optimization methods utilized in this domain. Furthermore, ML techniques and cryptographic algorithms are evaluated based on aspects such as accuracy, data security, computational efficiency, time consumption, and input aggregation for results. The integration of ML and virtualization has been shown to enhance techniques for cloud storage and access.*

Keywords: ***Cloud Computing, Cloud Computing Security, Machine Learning, Cryptography, Cloud service provider, Virtual machine, Particle swarm optimization.***

1. INTRODUCTION

The cloud makes it possible for users to access data and programs directly, as opposed to building, managing, and maintaining them on their hard drives or computers [1]. However, the power of cloud computing is also making its way into business enterprises. Due to its scalability and adaptability to changing needs, many companies and organizations have turned to cloud computing for backup and recovery, server and client security, recovery plans, software development, research, and customer-facing services. The most popular type of cloud computing is software as a service (SaaS), which removes the need for clients to install software on their computers, saving corporate IT staff time and money [2]. Additionally, you can customize your computing experience by using infrastructure as a service (IaaS). The fundamental IT infrastructure is assumed, and the required building pieces can be added. This plan should be chosen by businesses that already own a software company but require resources to sustain expansion in the future [3]. Developers can now realize their ideas with the help of Platform as a Service (PaaS). Both specialized and development tools are widely available. PaaS providers handle back-end concerns including infrastructure, security, and data integration. As a result, testing, adoption, and application development may be completed more quickly and affordably.

Cybersecurity pertains to cloud security in an environment that uses clouds. Preserve the security and privacy of online resources, apps, and gadgets. There are roles for individuals, small and medium-sized enterprises, and huge companies [5]. Using technology, standards, and procedures is necessary to secure cloud computing environments, cloud apps, and cloud data. It's critical to understand what to offer and how to offer it while offering cloud services. Ensuring that only authorized individuals have access to data and records stored in the cloud is a critical component of cloud security. In the end, data saved in the cloud must be protected by the cloud storage provider. The

cloud is extremely sensitive to transferred data. Sending a request to a place or moving files from one storage to another is simple. As a result, cloud end-to-end encryption is a fantastic choice for safeguarding private information. End-to-end encryption ensures that no one can read messages sent or received without the encryption key.

Using technology, standards, and procedures is necessary to secure cloud computing environments, cloud apps, and cloud data. It's critical to understand what to offer and how to offer it while offering cloud services. Ensuring that only authorized individuals have access to data and records stored in the cloud is a critical component of cloud security. In the end, data saved in the cloud must be protected by the cloud storage provider. The cloud is extremely sensitive to transferred data. Sending a request to a place or moving files from one storage to another is simple. As a result, cloud end-to-end encryption is a fantastic choice for safeguarding private information. End-to-end encryption ensures that no one can read messages sent or received without the encryption key [8].

The cloud is currently being used for communication, storage, and cloud computing. Nevertheless, if machine learning (ML) were included into the cloud, its capabilities would be substantially increased. An intelligent cloud can investigate, forecast, and analyze scenarios using all of the data stored in the cloud. Tasks will be finished much faster as a consequence of this [9]. Although machine learning is a relatively new technology, cloud computing and ML are both expanding fields. On the other side, cloud computing provides customers with the security and storage needed to access these ML-created apps. The requirement for resources creates a direct connection between cloud computing and machine learning. An ML algorithm requires a large amount of processing power, storage capacity, and concurrently operating servers. Subsequently, cloud computing is a significant factor in the production of new servers. Computation is the primary use of cloud computing. Since not everyone has access to numerous powerful computers, sample data for machine learning takes a lot of processing power. ML occasionally discovers storage and scheduling methods in cloud computing [10].

The process of transferring data, apps, and other business components into a cloud computing environment is referred to as "cloud migration". Applications and data can be moved via one cloud platform to another, as well as from one standardized environment to another, as part of a cloud migration [11]. Cloud architectures might not always have been a good fit for the architecture or design process. Because of this, it's possible that they need to be changed before they can be moved to the cloud.

This papers primary highlights are as follows:

1. It emphasizes the steps or procedures that cloud security must take into account when storing data utilizing cryptographic algorithms, machine learning techniques, and optimization strategies.
2. It offers a comprehensive review of the literature on the subject of safe cloud storage employing a range of methods, including machine learning, encryption, and optimization strategies developed by different researchers.
3. It also identifies the key findings and specifications for the ML and cryptography techniques used for the effective cloud data storage through comparison study.

The following sections make up the manuscript. The first section contains definitions for cloud computing, storage, and migration. In the second segment, the security and storage procedures incorporating machine learning techniques were further upon. Section 3 has mentioned the work done by others in the topic of safe cloud storage. part 4 presents a comparative examination of different methodologies based on cryptographic approaches and machine learning methods. The part that follows contains the conclusion and recommendations for further work.

2. Methods and Approaches Related to Cloud Computing

This portion of the article highlights the many steps and concerns that are taken in relation to cloud security. It discusses security issues in terms of cryptographic precautions and ML-based methods for implementing them. In addition, the optimum approaches and their corresponding needs have been emphasized.

2.1. Safety Measures for Cloud

Using cloud computing has several benefits, one of which is the capacity to store programs and data on the cloud. It is growing in popularity as a result, however since the data is managed outside of the owner's authority, there is a security risk. It is challenging for businesses to securely store sensitive data, such financial and medical records, because unreliable cloud providers put such information at danger. Different companies are developing different cryptographic methods to strike a balance between security and performance. Various encryption techniques can be employed to integrate cryptography with cloud computing. The most popular choice among users is to encrypt data before transferring it to the cloud [12]. Since the data is encrypted before it leaves the company and can only be unlocked by the designated recipient using their decryption key, it is regarded as more secure. Certain providers encrypt the data as soon as they get it. By default, encryption is used to secure data transport and storage.

A cryptographic technique is used to encrypt data, rendering it unintelligible to everyone save the intended recipient. Data is encrypted or decrypted using this algorithm. Encryption techniques are a vital component of cloud security tools. Data must be transformed mathematically in order to encrypt it. An algorithm is employed to convert the encrypted text into legible text, and a key is required to decode it. Here are a few techniques that are emphasized as being used for cloud security.

Data Encryption Standard: This symmetric key technique is used to encrypt digital data. All data streams are encoded and decoded using the same secret key. Permuting the 64-bit plain text to give it a new shape is the first stage in this process. The Feistel cipher, which encrypts data using 16 Feistel rounds, is used by DES. Every round uses the 48 bit round keys for plain text. These round keys are generated from sixty-six cipher keys. These sixteen 48-bit keys are then utilized. As a consequence, it produces a 64-bit cipher text [13].

AES: The most popular symmetric encryption technique interprets 128 bits of raw text by transforming it to 16 bytes. Use of a four-row, four-column matrix is necessary for data operations like replacement and permutation. A key controls how many transformation rounds are used when encrypting data.

RSA: Due to its asymmetric nature, it uses a range of key values and data block sizes. It can create public and private keys for encrypting and decrypting data with just two prime numbers. This method can help with authentication and communication security in open communication networks [13].

Blowfish algorithm: This method enables the encryption of 64-bit blocks with different key lengths and 16 rounds. It hasn't yet been the target of cryptanalysis and has a respectable encryption rate. It is free for the public to use because it is an open-source cipher block that is fast and secure.

Homomorphic algorithm: This approach involves the client and the service provider encrypting the data. When data is transmitted between the user and the service provider, it eliminates data risks and hides the plain text as coming from the provider, enabling the

providers to work solely with encrypted text. This technique can be used to shield a challenging mathematical process from the service provider [15].

Before data is provided to authorize users on their local devices, it is secured by cloud encryption solutions while it is being sent to and from a cloud-based service or storage. On a cloud storage device, data can be encrypted before being saved. Each method makes use of key-based cryptography to keep others from accessing data kept in the cloud.

2.2. Cloud based Secured Data Storage Practices

Cloud storage makes it feasible for an organization to store data offsite instead of on-site. This approach stores data on a third-party server, which employees can access on-demand from any device at any time. Files that are uploaded to the cloud are more susceptible to emerging attack methods. Cloud storage security is a shared responsibility between service providers and customers. If only one party has sufficient security measures in place, then data breaches and other dangers are more likely to occur. The following strategy should be used when it comes to cloud storage security: either baseline frameworks should be implemented on the platforms of the providers. To safeguard cloud data, customers must improve their native frameworks with extra security measures.

You may increase the security of your cloud storage by implementing some of the following techniques:

Data Encryption: Cloud service providers mandate the encryption of cloud data. Jumbled data can only be found by rogue software or someone attempting to access a file. A decryption key is the only tool needed to decipher data. For a company, client-side encryption can increase the security of cloud storage. Both encryption and decryption happen on the device of the intended user. Since the vendor does not own any encryption keys, decryption is not feasible. Even if a hacker gains access to the provider's server, the decryption key remains secure.

Two-Factor Authentication (2FA): It takes two pieces of information for a user to enable 2FA when they log in. 2FA requires the employee to provide an additional credential in addition to their login and password. 2FA adds an extra degree of security to stop hackers from accessing cloud storage using a stolen password [17].

Backups of data: The cloud provider must to regularly backup the data of its clients. The supplier should regularly build cloud data backups and distribute files among multiple data centers. In the event that one of the servers goes down, the client will not be impacted. A copy of all important cloud-based data should also be saved on a hard drive. Make sure these backups are updated on a regular basis and are unchangeable.

Create a Cloud Storage Policy: You may ensure that employees understand the organization's cloud storage and management policy by creating a cloud storage strategy. When your company's needs and the cloud services your employees utilize change, this document should be updated as well. Standards for using cloud storage, such as when and how to utilize it, should be included in a policy along with any customizations that may be required [18].

Cloud Storage Monitoring: By using continuous change, access, and activity monitoring, cloud storage security threats can be identified and removed. The majority of cloud storage companies provide thorough cloud monitoring, which includes alerts for file deletion and data exchange, among other things.

A policy-based control over who may access firm data in a cloud storage environment is necessary, as is a detailed awareness of how and where data is being moved to and from the cloud. Businesses should make sure that cloud storage security solutions offer accurate control over file movement based on web browser and operating system issues

while assessing them. As a result, it adds security features to cloud-stored data and automatically encrypts critical data as it is transferred between devices.

2.3. Cloud-Based Machine Learning Based Measures

Businesses may remain productive by using machine learning (ML) to identify threats and vulnerabilities in cloud platforms and apps, such as suspicious login activity, geographic abnormalities, and IP identities. Using standard cloud security solutions to protect data in cloud storages requires a lot of hard-coded limitations, continuous monitoring, and user intervention. This tactic is no longer as successful because of the exponential growth of data stored in public clouds. Strong substitutes for conventional techniques include automated control, ML-based insight generation, and predictive analytics. A prime example of this machine learning innovation is Amazon Macie, an ML system that Amazon uses to protect data in their S3 storage. The system dynamically analyzes data access attempts and detects various irregularities including large-scale data downloads, unusual login attempts, or unexpected data movement.

While machine learning models offer a range of methods for issue solving, they are not all created equal. Most cloud providers, including Google Cloud Platform (GCP), Amazon Web Services (AWS), and others, allow three fundamental types of predictions [19].

Binary predictions: Here, the emphasis is on Yes/No queries. It can help identify fraudulent orders and determine if a customer should be "upsold" a product based on recommendations from machine learning (ML) systems.

Prediction for category: It suggests that one is capable of classifying and analyzing a set of facts using information that has already been acquired. When working with a variety of data kinds and needing to apply a category to make the data easier to comprehend and process, this is useful.

Value predictions: Not only are they harder, but they also provide greater insight. quantitative forecasts made using information gleaned by applying learning algorithms to identify patterns in huge datasets.

Large quantities of data are used to train machine learning algorithms. Whether the data is structured, unstructured, or raw, powerful CPUs and graphics processing units are needed to process it. Today, only the best combination of private, public, and hybrid cloud systems can deliver massive processing capacity (depending on security and regulatory issues).

3. Related Work

Numerous researchers have previously focused on cloud security and put forth a number of methods to safeguard data in the cloud through the use of ML and cryptographic approaches. In this section, some notable works have been emphasized in several subsections focused on particular themes.

3.1. Related Work in Secure Cloud Computing

The authors claim that because cloud computing can pool resources, it is an emerging technology that can meet the demands of users in remote locations [21]. Although several frameworks for improving cloud computing security are discussed in this work, CPU consumption has not grown to keep up with the additional CPU usage needed to apply the different encryption algorithms. Therefore, a framework that can provide higher encryption with less effort is still needed. The authors have provided a model that may be helpful for a variety of cloud users with regard to security, and it is based on research into various security issues in cloud computing. The authors of [22] provide a framework that

includes the most important protocols for cloud computing privacy in the healthcare sector.

The best security practices for cloud-based healthcare systems are identified by considering the main risks connected to cloud computing and the sensitive data it handles. These best practices start with an overview of general information security risk management processes derived from the ISO 27000 family of standards. When using cloud computing, a health care organization needs to focus on risk assessment, mitigation plan, outsourced control, and requirement gathering processes. Maturity in particular is necessary for these processes.

When it comes to cloud computing, one of the hardest tasks to do is security. It is possible for both the application and the actual hardware to be attacked. An architecture that incorporates secure data transmission, storage, and usage in a semi-trusted cloud infrastructure can provide safe data interchange in the cloud. In [23], the authors demonstrate how to protect user processes through the use of a virtual machine monitoring system and the Kerberos system. In a cloud context, the framework employs a protocol to protect data while it travels from server to server. Sensitive client information is securely shared and well-protected when using the framework. The survey study discusses a research of potential solutions for cloud security issues [24]. Since 2008, many people have accepted the cloud as a reliable hosting option. Nonetheless, there's a perception that higher rates of commercial use will require much better cloud security. Previous studies have found that many of the issues that cloud computing confronts need to be resolved very now. According to recent research, the industry recognizes that methodology provides the best procedures and approaches for creating services and systems that are built to be resilient, long-lasting, and secure. More research is required to give these best practices for a broad range of applications and usage situations.

One of the primary security issues with the cloud computing concept is the pooling of assets. Cloud service companies have an incentive to inform customers about the security of their cloud. Concepts related to cloud computing, security challenges, and research difficulties are first covered in the paper [25]. Data security in cloud computing is a major worry. Apart from network and virtualization security, there are several more scenarios that are crucial for safety. These kinds of cloud computing issues have been highlighted by this research. The architecture of the cloud requires both the creation of fresh, enhanced security measures and the adaptation of already-existing ones. In order to maximize security and preserve a safe system, access privileges to cloud real-time data processing are reduced based on user location [26]. In order to maintain user comfort and achieve the goals of the research, tickets are issued using SSO agents, and resource access rights are managed according to each ticket's security grade to avoid abuse. Additionally, the safeguards put in place to aid improve protection keep the intended system safe from the numerous security risks.

Service disruption poses a significant risk to cloud security due to attacks such as denial of service, service hijacking, and VM-level breaches, according to authors in [27]. The study also addresses other risks and weaknesses related to improper use, unauthorized access, unsecured interfaces, and multi-tenancy cloud computing. The details of these dangers and how to mitigate them are also covered. Techniques for encryption and decryption are among these features. Security measures have been tested on a local PC as well as on the Google cloud platform. The local and cloud implementations of these algorithms' performances are contrasted. According to another study, data in cloud computing is collected and saved on a distant server by using the applications of the Cloud Service Provider (CSP) [28]. Since data is sent via media to a remote server, security must be provided. Prior to using cloud computing within an organization, security issues must be resolved. The writers of this book concentrate on problems with

and remedies for cloud computing security, or CSS. Data may be protected from hackers with the use of encryption.

3.2. Related Work in Secure Cloud Computing through Cryptography

Right now, there are a number of security issues with cloud computing. Users can store data in the cloud and then move it across other cloud services. Users' privacy is in jeopardy due to the most recent data management. Concerns concerning data security and virtualization impede cloud computing privacy since customers are primarily concerned about the protection of their personal information. The main emphasis here is on using elliptic curve encryption to offer data confidentiality and authentication across clouds [29]. Encryption techniques play a major role in cloud data security. An analysis of several factors in algorithms revealed that AES takes the least amount of time to encode cloud data. The Blowfish algorithm uses the least amount of memory. The DES algorithm requires the fewest steps to decrypt. RSA requires the greatest memory space and takes the longest to encrypt. All methods have been built using the IDE and JDK 1.7 to obtain the required results for cloud computing information.

Data security in the cloud has become a major problem. To improve data security, a random encryption process is used, per [31]. It must have been shown that when data is encrypted using a random key, the attacker may get perplexed about the content of the encrypted text and therefore be unable to identify whether two encoded messages, even if they have the same key, correspond to the same plaintext. Although there are many security risks, the security of data stored on the cloud and the privacy of information while it is being supplied by the CSP are two of the most urgent issues. A variety of security-related issues are covered in [32], with an emphasis on data security and encryption methods. Just two of the block cipher techniques being researched as potential solutions to the cloud security issue are RSA and Blowfish. Similar to this, the authors of [33] selected AES and RSA as the best compatible security algorithms. Their multilayer encryption approach encrypts data using AES algorithms at first, and then uses RSA methods to encrypt the first-level output before uploading it to cloud storage.

According to the authors in [34], their framework can be utilized with the primary capabilities of cloud computing. It includes a built-in One-Time Password (OTP) system. Within this model, Elliptic Curve Cryptography (ECC) is used to protect clients and cloud storage systems. The main emphasis is on enhancing the security mechanisms of the entire cloud computing platform. To encrypt encoded data and store it with a third-party Cloud Service Provider (CSP), the author applied cryptographic techniques such as the Symmetric Key Based Encryption (SKBE) approach [35]. The SKBE concept can also be employed to secure the cloud.

By utilizing cryptography and steganography, the challenges related to cloud storage data security can be addressed. The authors of [36] recommend using the RC6, 3DES, and AES methods to secure data, with the LSB approach ensuring the safe storage of sensitive information. This method allows for faster encryption and decryption operations. The proposed security approach enhances data integrity, provides high security, ensures low latency identification, and maintains confidentiality. In [37], the authors introduced a novel encryption scheme by replacing the AES algorithm's static S-box with a dynamic S-box. Additionally, the generated keys are encrypted using RSA and Blow fish techniques to ensure anonymity. They compared these methods with existing symmetric key methods like DES, 3DES, and RC2 to evaluate their effectiveness.

Cloud computing hassles high computational hustles, making complex cryptography techniques impractical. To address this, the authors in [38] utilized an improved Blowfish method combined with an Elliptic Curve Cryptography (ECC) technique. This approach improves security and efficiency by using Blowfish to encrypt the data and ECC to decrypt the key. Additionally, data integrity is maintained through the use of digital

signatures. This method has demonstrated improvements in throughput, processing time, and memory usage. In another work [39], the authors employed Honey Encryption, which addresses some of the existing challenges in cryptographic data encryption while offering additional benefits to users. However, high computational and storage costs, along with complexity, remain drawbacks of current cryptographic encryption methods.

3.3. Related Work in Machine Learning-Based Secure Cloud Computing

The author's attempt to create a novel cloud security solution using ML approaches is shown in [40]. Convolution Neural Networks (CNNs) are a potent tool that may be utilized to boost security in the cloud environment by offering automated and responsive approaches. Cloud security is a main focus of this study. Artificial Intelligence (AI) can provide solutions that go beyond just identifying different trends in sensitive data to include full techniques for protecting firm data across all cloud apps. Since cloud data security is a key need for cloud outsourcing, a strong algorithm is required. Authors [41] provide a method for cloud security. This approach proposes two algorithms: machine learning and neural networks. The ML approach is based on a KNN-based neural network algorithm that uses hashing and data fragmentation. With both of these methods, cloud security is enhanced by encoding data at the cloud server.

The goal of machine learning is to automatically optimize algorithms through more usage. The study [42] discusses security issues, difficulties, and solutions that use one or more machine learning algorithms in depth. They examine several forms of learning as well as additional machine learning techniques to address cloud security issues. Then, they assess the characteristics, advantages, and disadvantages of each strategy to determine which works best. ML models are frequently trained on a single dataset, which leads to semantic gaps in the model's outputs and application. Research demonstrating the range of datasets and scenarios to which these models may be used is lacking. In the study, supervised machine learning models are trained using the UNSW dataset [43]. They then test these models on the ISOT dataset. Their findings indicate that further ML research is required before cloud security can benefit from it.

The authors put forth a secure cloud data security paradigm, according to [44]. The proposed architecture may address a number of cloud security concerns, such as data security from violations and defense against a forged authorized identity user. Data security and privacy are put at risk by a number of issues and concerns related to cloud computing. It talks about the risks associated with cloud data storage. Enhanced cloud data encryption is one advantage of the proposed CSS architecture. The OTP was developed by the authors in order to protect users and data collectors from unauthorized access to cloud storage.

3.4. Related Work in Optimization-Based Secure Cloud Computing

The accuracy of the IDS's detection is greatly influenced by the machine learning method that was employed to build it. Consequently, in order to improve the detection effectiveness of IDS for data security, a cuckoo optimization-based preprocessing method for network traffic data is proposed in [45]. When compared to other existing methods, the efficiency of the recommended approach is higher and its accuracy is lower. A unique method of data encryption that makes use of several key generation techniques may be found in [46]. Three types of keys are generated: a Pseudorandom Synthesis, an Improved Cipher Block Chaining (ICBC) hybridization, and a Memory-based Hybrid Dragonfly Optimization Algorithm (MHDA). Using a combination of the Particle Swarm Optimization Algorithm (PSO) and the Dragonfly Optimization Algorithm (DA) in MHDA, a new key is created for data encryption. For performance monitoring, MHDA outperforms DA and PSO optimization techniques.

PSO and genetic programming are the scheduling techniques that are most frequently applied in distributed systems, according to [47]. To reduce the amount of time needed for

this population to expand, hybridization is added to the standard PSO algorithm during the formation of the initial population. With this method, tasks in a cloud computing environment may be planned more effectively to take use of available resources, which will shorten the time needed to complete them. To address the security problems, the authors suggest in [48] a security-aware compute offloading technique. A very effective cryptographic algorithm has been created and proposed. This approach combines orthogonal learning PSO (OLPSO) with sanitation. Data confidentiality is enhanced and the key is produced using this method. Numerous assessment indicators are used to analyze and compare the performance of the proposed technique.

The Bird Swarm Optimization Load Balancing (BSO-LB) technique has been presented [49] as a solution, which views Virtual Machines (VMs) as target food patches and workloads as birds. In the cloud simulation, tasks are meant to be autonomous and non-preemptive. The algorithm under discussion aims to preserve system balance while simultaneously responding more quickly. The authors have combined the load balancing strategy with the binary variant of the BSO technique. To determine how successful the new strategy is, other load balancing algorithms such as MAX-MIN, RASA, and Enhanced PSO are compared and analyzed.

3.5. Related Work on Secure Data Storage in Cloud Computing

A summary of the most recent research on single and multi-clouds was provided by [50] in order to detect, prevent, and address problems. Many efforts have been made to ensure the security of single clouds and data storage in the context of cloud security, while multi-clouds have received less attention. splintering, redundancy. The author suggests scattering as a strategy for handling both inadvertent and deliberate mistakes. It is investigated how to use the FRS technique as an intrusion-tolerance tactic for cloud storage [51]. It is also recommended to explore the potential applications of CCS built on FRS in various scenarios. To demonstrate the idea's durability, they formalize their architecture, evaluate the technique's performance and security, and compare it to the industry standard model.

To guarantee data security, the Tornado codes method [52] combines symmetric cryptography with erasure codes. While a boot password is used to address the traditional data encryption problem of key conservation and promotion, an error-correcting hash based on Tornado code can be used to fix issues and recover lost data; the system's design leverages the corrective effects of Tornado data redundancy code deletion code. They have introduced the cloud storage system prototype, which is based on a reliable log and POR system. Similar work addresses CCS [53]. These cloud service providers are assigned the job of cracking the encrypted text file after being chosen at random. The user can decrypt the encrypted file by putting the right blocks back together.

Another study [54] proposes a system that utilizes AES and Fully Homomorphic Encryption (FHE) for secure data transport and recovery. AES ensures robust security by guarding against known vulnerabilities. This architecture also improves the accuracy and accessibility of customer data within the cloud. Similarly, recent advancements include the development of a secure cloud storage system based on a fog-based three-layer structure [55]. In this system, proactive measures are performed on a trusted fog server, and actual data is fragmented and distributed across multiple cloud servers. The proposed system integrates anti-tampering techniques such as homomorphic encryption, searchable encryption, CRH, and Block Administration. Homomorphic encryption allows secure outsourcing by segmenting and combining datasets into fixed-length blocks.

Researchers have explored resource scheduling and VM migration in several studies [46-50]. Additionally, various researchers have investigated the implementation of machine learning approaches for enhancing data security in the cloud [51-57].

Furthermore, notable contributions have been made in the realm of secure cloud implementation by authors [68-71].

4. Detailed Analysis

Many different types of organizations find cloud computing to be an appealing alternative due to its massive data storage capacity and quick processing speed. When hosting and retrieving data in the cloud, security is one of the main concerns. The majority of the work done on CSS has been focused on security and the use of ML techniques to improve speed. A comparative analysis of the several machine learning-based strategies for cloud security has been conducted, as shown in Table 1. The categorization is carried out according to variables such as the model type—supervised (S) or unsupervised (UN)—the method employed, the degree of accuracy attained, the security of the data, and the computing efficiency determined by the resource requirements. Because the great majority of programs that employ them follow the aforementioned parameters when they are being executed, they are considered crucial parameters for model analysis.

Table 1. Comparison of Machine Learning Techniques for Cloud Security Using Parameters

Reference Technique	Supervised (S) / Unsupervised (US)	Technique Used	Precision	Data Security	Computational Effectiveness
[4]	S	ANN	×	✓	×
[6]	S & US	SVM	×	✓	×
[57]	S	ANN	✓	×	×
[56]	S	KNN	×	✓	✓
[30]	S	ANN	✓	×	×
[20]	UN	CNN	×	✓	×

Based on Table 1, one may deduce that the Artificial Neural Network (ANN) was utilized in most of the strategies. In addition to ANN, a few other techniques are also in use, including CNN, KNN, and Support Vector Machine (SVM). Furthermore, it may be deduced that ANN-based methods are more accurate than other methods. However, because ANN-based approaches take more memory and time to deploy, their computational requirements are ineffective. The majority of methods address the problem of data privacy while uploading and disseminating data to the cloud.

Table 2 lists the approaches and methods for cloud security that have been built on cryptography, as well as the considerations that were used while evaluating the methods' performance. The third-party authentication of the user gaining access to the cloud, process features such as the use of a lightweight method, process time requirements, and throughput—the ultimate measure of success—are all taken into account in this case.

Table 2. Comparison of Cryptographic Techniques for Cloud Security

Reference Technique	Algorithm Used	Third Party for Cloud Verification	Lightweight Efficient	Time Efficient	Throughput Efficient
[37]	AES & ECC	×	×	✓	×
[38]	ECC & Blowfish	×	×	×	✓
[39]	Honeypot	×	✓	✓	×
[20]	AES	×	×	×	×
[16]	AES, RSA & SHA	✓	✓	×	×
[14]	AES	✓	×	×	×
[7]	RSA,DES & AES	✓	✓	✓	✓

5. Potential Directions

Data security poses a significant challenge in cloud technology, mitigated to a large extent by encryption techniques. Among these, homomorphic encryption stands out as the optimal method for safeguarding an organization's private data over public channels. Unlike traditional security mechanisms such as DES, AES, RSA, and Blowfish, homomorphic encryption operates directly on encrypted data, offering robust security measures. To enhance cloud data security further, it is imperative to develop and maintain machine learning (ML) algorithms. Although techniques based on Artificial Neural Networks (ANN) demonstrate superior accuracy compared to other methods, they often require substantial memory and time for implementation, posing computational challenges. AES is widely deployed in numerous approaches for securing cloud data, often combined with DES or RSA to facilitate efficient third-party cloud verification. However, many cryptographic techniques employed for securing the cloud suffer from inefficiencies in terms of time and resource usage. Looking ahead, statistical methods will play a crucial role in improving convergence and expanding optimization approaches in cloud resource allocation to conserve energy. Additionally, blockchain technology holds promise for revolutionizing cloud security and data center operations.

REFERENCES

[1] *Syed. Shanawaz Basha, N. Musrat Sultana. Multilayered Approach for Data Security in Cloud Storage. YMER, 23(6), 49-60.*

[2] *Tsai, W., Bai, X., & Huang, Y. (2014). Software-as-a-service (SaaS): perspectives and challenges. Science China Information Sciences, 57(5), 1-15.*

[3] *Shahzadi, S., Iqbal, M., Qayyum, Z. U., & Dagiuklas, T. (2017, June). Infrastructure as a service (IaaS): A comparative performance analysis of open-source cloud platforms. In 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.*

[4] *N. Musrat Sultana, K. Srinivas. Survey on Centric Data Protection Method for Cloud Storage Application. International Conference on Computational Intelligence and Computing Applications, 2021, IEEE..*

[5] *Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.*

[6] *Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018, April). Cyberattack detection in mobile cloud computing: A deep learning approach. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE.*

[7] *Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, June). Enhanced cloud data security using AES algorithm. In 2017 International Conference on Intelligent Computing and Control (I2C2) (pp. 1-5). IEEE.*

[8] *Wheeler, A., & Winburn, M. (2015). Cloud storage security: A practical guide. Elsevier.*

[9] *Pop, D. (2016). Machine learning and cloud computing: Survey of distributed and saas solutions. arXiv preprint arXiv:1603.08767.*

[10] *Gao, J., Wang, H., & Shen, H. (2020, August). Machine learning based workload prediction in cloud computing. In 2020 29th international conference on computer communications and networks (ICCCN) (pp. 1-9). IEEE.*

[11] *Zhao, J. F., & Zhou, J. T. (2014). Strategies and methods for cloud migration. international Journal of Automation and Computing, 11(2), 143-152.*

[12] *M. Madhavi, S. Shanawaz Basha, M. Ranjith Reddy, (2013, June). Secure Data Forwarding on Cloud Storage System, International Journal of Scientific & Engineering Research (pp. 1596- 1601).*

[13] *Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).*

[14] *More, S., & Chaudhari, S. (2016). Third party public auditing scheme for cloud storage. Procedia Computer Science, 79, 69-76.*

[15] *Geng, Y. (2019). Homomorphic encryption technology for cloud computing. Procedia Computer Science, 154, 73-83.*

[16] *Chakraborty, S., Singh, S., & Thokchom, S. (2018, August). Integrity checking using third party auditor in cloud storage. In 2018 Eleventh International Conference on Contemporary Computing (IC3) (pp. 1-6). IEEE.*

[17] *Soares, L. F., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2013, December). Secure user authentication in cloud computing management interfaces. In 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC) (pp. 1-2). IEEE.*

[18] *S. Kumar, M. S. Gaur, P. Sagar Sharma and D. Munjal, "A Novel Approach of Symmetric Key Cryptography," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 593-598, doi: 10.1109/ICIEM51511.2021.9445343Hemmat,R. A., & Hafid, A. (2016). SLA violation prediction in cloud computing: A machine learning perspective. arXiv preprint arXiv:1611.10338.*

[19] *Li, K., Gibson, C., Ho, D., Zhou, Q., Kim, J., Buhisi, O., ... & Gerber, M. (2013, April). Assessment of machine learning algorithms in cloud computing frameworks. In 2013 IEEE Systems and Information Engineering Design Symposium (pp. 98-103). IEEE.*

[20] *Zhao, X., & Zhang, W. (2016, July). An anomaly intrusion detection method based on improved k-means of cloud computing. In 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC) (pp. 284-288). IEEE.*

[21] *Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a security management in cloud computing for health care. The Scientific World Journal, 2014.*

[22] *Lanjewar, M. V., Dharaskar, R. V., & Thakare, V. M. An Approach towards Securing Data in Cloud Computing.*

[23] *Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.*

[24] *Anshika Negi, Mayank Singh and Sanjeev Kumar. Article: An Efficient Security Farmework Design for Cloud Computing using Artificial Neural Networks. International Journal of Computer Applications 129(4):17-21, November 2015. Published by Foundation of Computer Science (FCS), NY, USA*

[25] *Jang, E. G. (2019). System Access Control Technique for Secure Cloud Computing. Journal of the Korea Society of Computer and Information, 24(8), 67-76.*

[26] *Alrehaili, A., Mir, A., & Junaid, M. (2020). A Retrospect of Prominent Cloud Security Algorithms. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(3), 749-755.*

[27] *Zulifqar, I., Anayat, S., & Kharal, I. (2021). A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering & Electronic Business, 13(3).*

[28] *Ibrahim, A. A., Cheruiyot, W., & Kimwele, M. W. (2012). Data Security in Cloud Computing with Elliptic Curve Cryptography. International Journal of Computer (IJC), 26(1), 1-14.*

[29] *Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. International journal of engineering research and applications, 3(4), 1922-1926.*

[30] *Aceto, G., Ciuonzo, D., Montieri, A., Persico, V., & Pescapé, A. (2019, June). Know your big data trade-offs when classifying encrypted mobile traffic with deep learning. In 2019 Network traffic measurement and analysis conference (TMA) (pp. 121-128). IEEE.*

[31] *Potteti, S., & Parati, N. A. M. I. T. A. (2015). Secured Data Transfer For Cloud Using Blowfish. International Journal of Advances In Computer Science and Cloud Computing, 3(2), 17-22.*

[32] *Ramadan, H., & Djamilou, M. A. (2017). Using Cryptography Algorithms to Secure Cloud Computing Data and Services. American Journal of Engineering Research (AJER), 6(10), 334-337.*

[33] *Hussain, A., Xu, C., & Ali, M. (2018). Security of cloud storage system using various cryptographic techniques. International Journal of Mathematics Trends and Technology (IJMTT), 60(1), 45-51.*

[34] *Sarkar, M. K., Das, R., & Dhaka, V. S. A Symmetric Key Based Framework for Data Security in Cloud Computing.*

[35] *Sharma, V., Chauhan, A., Saxena, H., Mishra, S., & Bansal, S. (2021, October). Secure File Storage on Cloud using Hybrid Cryptography. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). IEEE.*

[36] *El-Attar, N. E., El-Morshedy, D. S., & Awad, W. A. (2021). A New Hybrid Automated Security Framework to Cloud Storage System. Cryptography, 5(4), 37.*

[37] *Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6).*

[38] *Jain, R., Yadav, S., & Khan, A. A. (2021). Secure Data Transfer Based on Cloud. Annals of the Romanian Society for Cell Biology, 19307- 19313.*

[39] *S. Kumar, G. Karnani, M. S. Gaur and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 599-604, doi: 10.1109/ICIEM51511.2021.9445377.*

[40] *Khan, M. A Cloud Security Model Based On Machine Learning and Neuron Network.*

[41] *Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.*

[42] *San, A. J. (2021). Cloud Security using Supervised Machine Learning. International Journal of Advanced Scientific Innovation, 2(4).*

[43] *Sauber, A. M., El-Kafrawy, P. M., Shawish, A. F., Amin, M. A., & Hagag, I. M. (2021). A New Secure Model for Data Protection over Cloud Computing. Computational Intelligence and Neuroscience, 2021.*

[44] *Singh, D. A. A. G., Priyadharshini, R., & Leavline, E. J. (2018). Cuckoo optimisation based intrusion detection system for cloud computing. International Journal of Computer Network and Information Security, 9(11), 42.*

[45] *Kaleeswari, C., & Kuppusamy, K. Memory Based Hybrid Dragonfly Optimization for Multiple Key Generation using Cloud Computing.*

[46] *Abraham, A., Mauri, J. L., Buford, J., Suzuki, J., & Thampi, S. M. (Eds.). (2011). Advances in Computing and Communications, Part I: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011. Proceedings (Vol. 190). Springer Science & Business Media.*

[47] *John, N. P., & Bindu, V. R. An Optimal Sanitization Algorithm Based Secure Migration of Virtual Machines in Cloud Datacenters.*

[48] *Mishra, K., & Majhi, S. K. (2021). A binary Bird Swarm Optimization based load balancing algorithm for cloud computing environment. Open Computer Science, 11(1), 146-160.*

[49] *Sujana, B., Tejaswini, P., Srinivasulu, G., & Karimulla, S. (2013). Secure Framework for Data Storage from Single to Multi clouds in Cloud Networking. Int. J. Emerg. Trends Technol. Comput. Sci, 2(2).*

[50] *El Mrabti, A. A., Ammari, N., & De Montfort, M. (2016). New mechanism for cloud computing storage security. (IJACSA) International Journal of Advanced Computer Science and Applications, 7(7).*

[51] *Wang, R. (2017). Research on data security technology based on cloud storage. Procedia engineering, 174, 1340-1355.*

[52] *Selvakumar, K., & Prabakaran, M. Data Protection Framework for Secure Storage in Cloud Computing.*

[53] *Ravindranath, K., Reddy, M. S., Reddy, M. D., & Chaitanya, D. Secure Data Storage and Retrieval in the Cloud.*

[54] *Ahsan, M. M., Ali, I., Imran, M., Idris, M. Y. I., Khan, S., & Khan, A. (2019). A fog-centric secure cloud storage scheme. IEEE Transactions on Sustainable Computing.*

[55] *Strumberger, I., Bacanin, N., Tuba, M., & Tuba, E. (2019). Resource scheduling in cloud computing based on a hybridized whale optimization algorithm. Applied Sciences, 9(22), 4893.*

[56] *Kumar, R. S. S., Wicker, A., & Swann, M. (2017, November). Practical machine learning for cloud intrusion detection: challenges and the way forward. In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security (pp. 81-90).*

[57] *Park, J., & Lee, D. H. (2018). Privacy preserving k-nearest neighbor for medical diagnosis in e-health cloud. Journal of healthcare engineering, 2018.*