


Review Article

PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud

John Kwao Dawson ¹, **Frimpong Twum**,² **James Benjamin Hayfron Acquah**,²
and **Yaw Marfo Missah**²

¹*Sunyani Technical University, Department of Computer Science, Sunyani, Ghana*

²*Kwame Nkrumah University of Science and Technology, Department of Computer Science, Kumasi, Ghana*

Correspondence should be addressed to John Kwao Dawson; kwaodawson1@yahoo.com

Received 6 January 2023; Revised 13 June 2023; Accepted 23 June 2023; Published 3 July 2023

Academic Editor: Shadab Alam

Copyright © 2023 John Kwao Dawson et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Industries have embraced cloud computing for their daily operations due to the volume of data they create. As data generation and consumption have increased, the challenges and opportunities have also increased. Researchers have proposed various cryptographic schemes to secure data on the cloud. Regardless of the multiple cryptographic schemes proposed, security remains an obstacle to cloud computing's widespread adoption. Also, these cryptographic schemes' run times are proportional to data sizes, motivating excessive CPU engagement during execution of huge data, which has consequences for the need for high bandwidth to transfer data to the cloud. This systematic review tries to uncover the most often used cryptographic schemes and their run time trends to attain confidentiality and privacy of cloud data. The study considered published articles from well-known databases such as Taylor & Francis, Scopus, Research Gate, Web of Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, Sage, Emerald, Wiley Online Library, and ACM from 2016 to 2022. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines were used to select 73 published works for this study using keyword searching. Data security and cloud security were the security challenges that received the greatest attention in the study with encryption techniques as the most common solution. From the study, 90% of the schemes used to secure data on the cloud produced linear run times. The investigation discovered that nonlinear symmetric stream cipher methods were infrequently employed to protect the secrecy and privacy of cloud data.

1. Introduction

As data production and utilization have expanded, so have the difficulties and opportunities. To preserve this massive amount of data, a paradigm shift in data storage, security, integrity, and availability is required [1]. The use of cloud computing can help solve these issues. Cloud computing is the delivery of computer services through the Internet on a pay-as-you-go basis [2].

The use of cloud computing enables the use of software and infrastructure anywhere on the earth, with all services administered by cloud service providers [3]. Cloud computing has been on the agenda of organizations and governments throughout the world in order to achieve lower

operating costs and flexibility of data capabilities, which are believed to be the greatest information technology solutions [4]. The adoption of the cloud by governments and businesses has resulted in the emergence of several service providers such as Salesforce, Amazon, and Yahoo, with many suppliers such as IBM and Oracle offering database technical support [5].

Despite the multiple benefits and the drive by other organizations to contribute to the sustainability of cloud computing, data security remains a key concern [6]. This is due to the various cloud computing architecture and designs, such as software, hardware, and application programming interfaces [7]. However, because of this disparity in setup, cloud customers and providers face a variety of

security challenges [6, 7]. This is seen in [8] where Imperva warns clients to be on the lookout for a new attack on cloud services known as man-in-the-cloud.

1.1. Services and Cloud Deployment Models. This section provides an overview of the various cloud computing service models and a quick assessment of the subject at hand.

1.1.1. Software as a Service (SaaS). Software as a service refers to the practice of a third party providing software to several tenants on a pay-per-use basis. Clients from small and big enterprises can access these systems, which only require the deployment of software once. An integrated system that is always in use on the internet may call for both routine modifications and innovative activities [9].

1.1.2. Platform as a Service (PaaS). Platform as a Service [10] provides an environment that permits the creation, development, and maintenance of applications. The produced apps may be immediately planned, improved, and evaluated by the cloud customers, and the development cycle of the applications can be tracked.

1.1.3. Infrastructure as a Service (IaaS). All other cloud services are based on the foundation of Infrastructure as a Service as indicated in Figure 1. In the typical network design, this takes the role of conventional data centers. This concept is used by cloud service providers to offer platforms on which cloud clients may store their resources [11]. Resources from cloud customers are transferred to IaaS on the assumption that the cloud service provider can maintain the level of service they offer. The service-level agreement (SLA), which is connected to the lifespan of the cloud service provider and exhibits the financial as well as procedural dynamism related to SLA, serves as a guarantee for the use of IaaS.

1.1.4. A Container as a Service (CaaS). Developers that utilize this service use a package for all of their programming needs. The container includes all of the coding requirements, run time, and configurations needed for the system to operate on a host computer [12]. The libraries required to run a program are all provided by a container as a service, which eliminates the need for additional virtual systems to supply the necessary libraries as shown in Figure 2. For uploading, setting up, running, scaling, and maintaining the container, they can offer a complete unit.

1.2. Cloud Deployment Models. The distinctiveness of gaining access to shared resources in the cloud is determined by the deployment models in cloud computing. Based on this, four models are taken into consideration.

1.2.1. Public Cloud. According to their shared objective, this kind of cloud enables entities to access data over the internet and makes programs accessible to the group with the aid of

cloud servers [13]. These clouds are made available to the public at large, are managed by governmental bodies, companies, academics, or a combination of all three, and are hosted by a cloud service provider on their website [14].

1.2.2. Private Cloud. Private clouds, according to the authors in reference [15], are designed to be used by businesses to carry out work or store employees' details. Such a cloud platform is trademarked since it specifically saves the entity's extremely sensitive data. Private clouds are utilized as a single entity scheme, and they operate using either new resources or existing technology that is housed on the organization's hardware but is managed by a different firm [16].

1.2.3. Hybrid Cloud. A hybrid cloud is created by combining the strengths and weaknesses of public and private clouds, which has the benefit of improving data security for both infrastructures [17]. Hybrid clouds, according to the authors in [18], assert that their integration calls for a higher level of technical expertise in terms of data gathering, analysis, evaluation, and overall management of hybrid platforms. Hybrid clouds provide several challenges including data governance and security.

1.2.4. Community Cloud. This is a sort of hybrid private cloud and is regarded as a multitenancy platform designed to let businesses use a shared resource [19]. Because they are utilizing the community software to accomplish a single objective, this enables the users to cooperate on a shared project as shown in Figure 3. On this platform, clients are all concerned with shared security as well as the guiding principles of agreement with the delegation of oversight and evaluation to a third party [21].

1.3. Cloud Client. Cloud customers are people or businesses who make use of a cloud service provider's resources. They have the absolute right to select the service of their choice and to pay for the services that the service provider really provides to them before their contract expires. The cloud customer establishes a service level agreement to specify how well the service will be provided [22]. These contracts are signed in relation to service quality, privacy, security, and integrity.

1.4. Cloud Service Providers. The term "Cloud Service Provider" (CSP) refers to organizations that provide cloud clients with computing as a service. Cloud service providers are in charge of overseeing the management of all cloud services and infrastructure [23]. In Software as a Service (SaaS) and Infrastructure as a Service (IaaS) platforms, the cloud service provider is responsible for organizing, arranging, maintaining, and keeping up-to-date applications as well as managing infrastructure in order to give resources to cloud customers. All of the architectural planning and computer infrastructure, including networks, servers, and infrastructure hosting, are provided by the cloud service

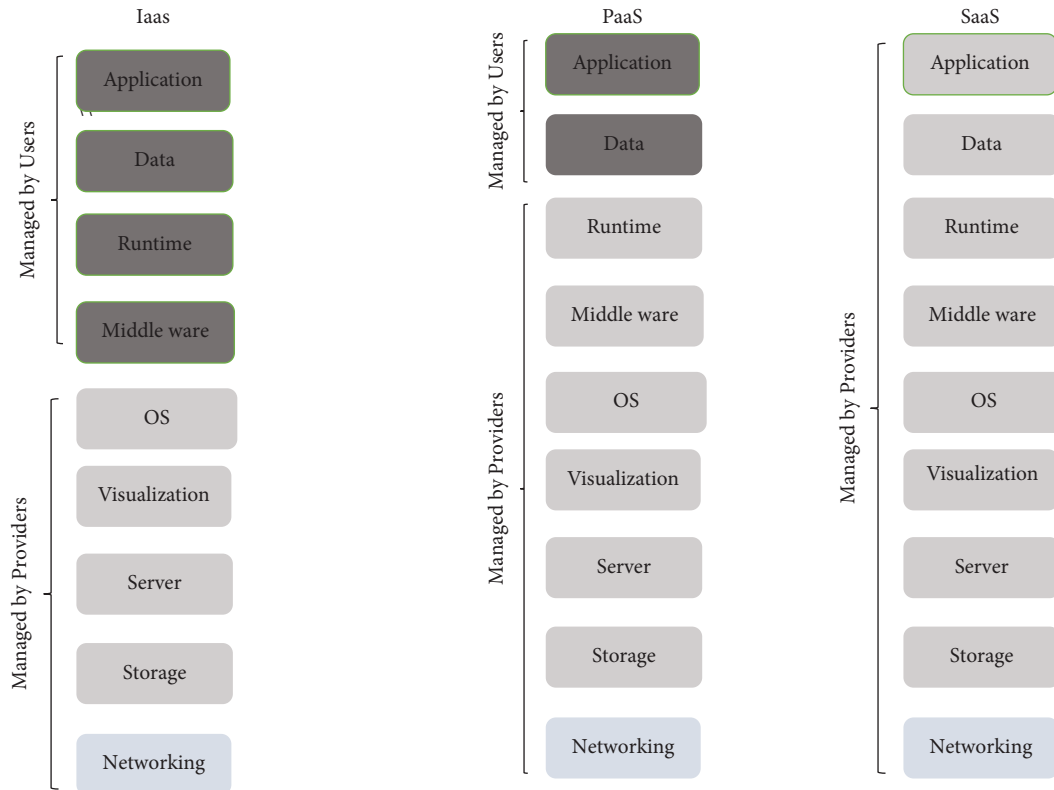


FIGURE 1: Management of resources in cloud computing [6].

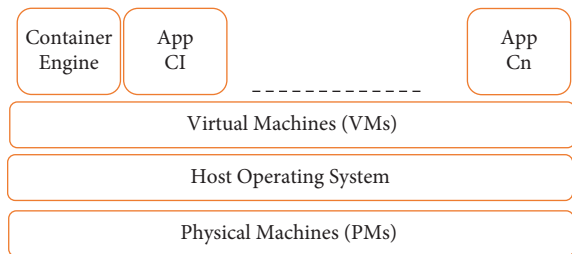


FIGURE 2: Container as a service architecture [12].

provider [24]. A detailed functionality of performers in the cloud is depicted in Table 1.

1.5. Security Challenges in Cloud Services

1.5.1. Security in Software as a Service. The cloud computing interaction layer is represented by this. Therefore, all security concerns are data based [26]. This is because, at this point, it is up to the cloud client to ensure the necessary security for the data off-loaded by implementing checks on who may access such data as well as the security measures used by the cloud service provider. The most frequent security concerns relating to software as a service are lack of control, access management, data privacy, and continuous monitoring. Due to the aforementioned problems, it is crucial to take into account how cloud providers and SaaS providers relate to one another in terms of security. This necessitates careful examination of the suppliers' security measures.

1.5.2. Security in Platform as a Service (PaaS). There are three layers for the platform as a service, according to [27]. The layer that connects to software as a service, the middle layer is intended for application storage, and database data run timing management, and the last layer is for back-end operations including network, storage, and CPU storage. The security concerns are data breaches and security controls as suggested by [28]. As a result of these security concerns, cloud service providers need to make sure that adequate identity and verification processes are in place for PaaS.

1.5.3. Security in Infrastructure as a Service (IaaS). To store their data and optimize their CPU and other functions, cloud clients employ virtual devices at this service level. Based on how frequently the service is accessed, this layer has several security problems. Security issues that have been raised include denial of service attacks, limited control, and compromised identity [29]. This necessitates the establishment of appropriate legal provisions and guidelines for cloud clients using IaaS.

1.5.4. Security in Container as a Service (CaaS). Because of benefits such as being light, quick, easy to deploy, improved resource usage, and version control, the adoption of containers as a service has expanded [30].

The following are a few security issues with CaaS [30]: well construction of container images and requiring new security methodology. Since clients are permitted to share

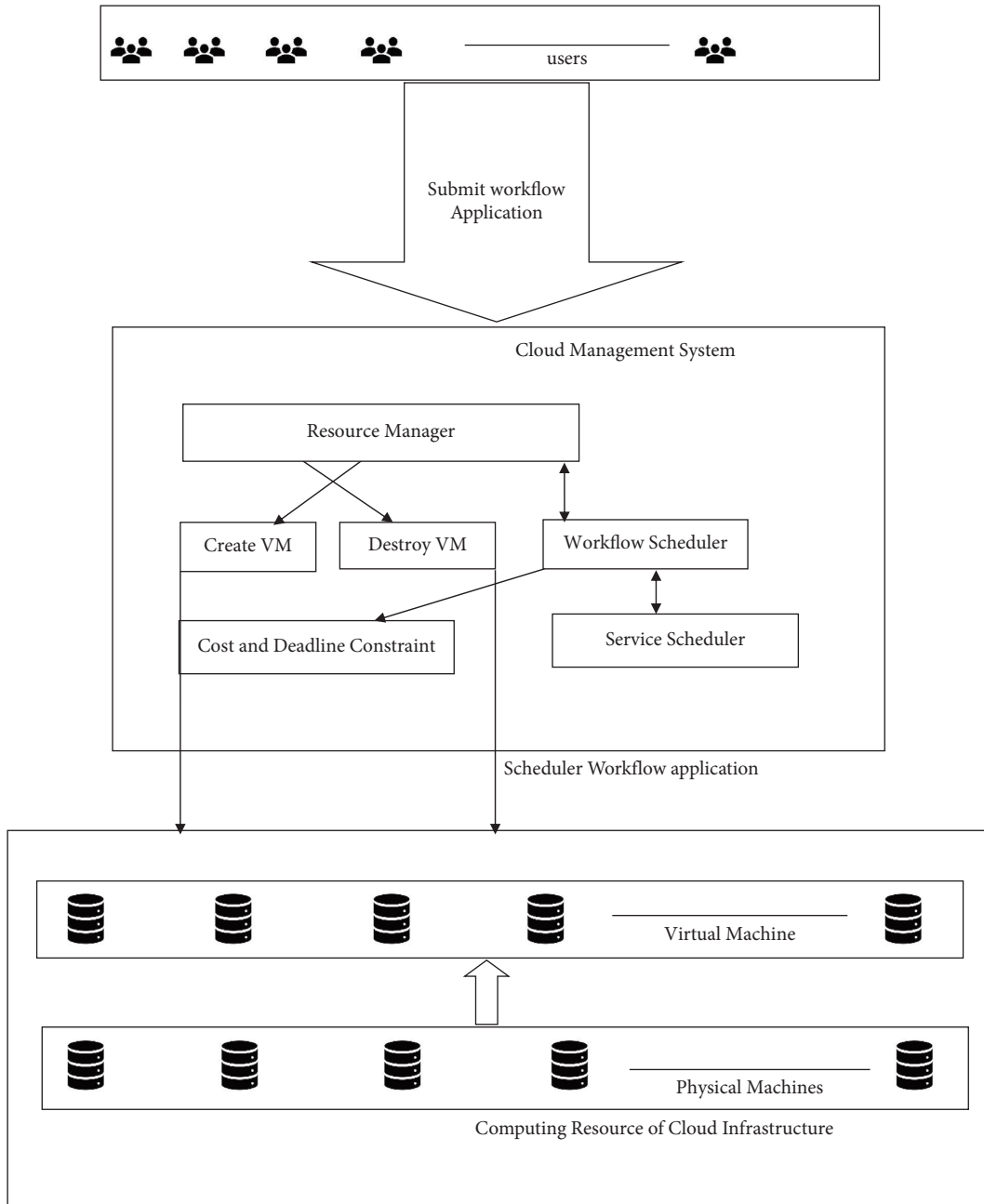


FIGURE 3: Scheduled workflow on a community cloud [20].

TABLE 1: Various performers in cloud computing [25].

Performer	Function
Cloud client	An entity that uses the services rendered by a cloud service provider based on pay as you use
Service provider	Any company that renders computing service to cloud clients via the internet and ensures the provision of resources the clients require to attain the satisfaction desired
Cloud auditor	This is a third-party responsible for the evaluation of services rendered to a cloud client. This is in the form of assessing performance, system operation, and security
Broker of cloud	An entity that mediates between cloud client and cloud service provider seeing to quality service and delivery
Carrier of cloud	They ensure connectivity between cloud clients and cloud service providers for the transport of cloud services

the same OS, the OS kernels must be more secure to make Container as a Service more secure. The security issues with the different cloud services are indicated in Table 2.

1.6. Cloud Security Issues

1.6.1. Confidentiality. Confidentiality is the prevention of unauthorized parties from accessing data [31]. To accomplish this, several researchers have employed a variety of strategies, ranging from cryptography to the combination of encryption and block division [32]. Examples of security measures implemented to protect data confidentiality include the following:

(1) *Encryption Using a Biometric Approach.* This method makes use of a variety of factors, including speech transmissions, eye iris readings, facial recognition, and fingerprint scans. To obtain access to the stored data, these systems are quite different and challenging to modify [33].

(2) *Using the Classification Approach of K-NN.* This is one of the most sophisticated methods for ensuring data security, and it is regarded as a supervised machine-learning method [34]. This is frequently used in pattern recognition, data segmentation, forecasting, and approximation with the goal of choosing insightful data that enables data secrecy.

(3) *A Secure Scheme Using HPI.* By utilizing HTTP's (hypertext transfer protocol) security protocol, this method enables cloud clients to store data in the cloud [32]. When the data are requested, they are unscrambled after being scrambled and transferred to the cloud. Because of this, the end encryption strategy increases secrecy.

1.7. Integrity. Data integrity guarantees the accuracy of clients' data by demonstrating that their data are secure and have not been altered using the right cryptographic algorithms [35]. Data integrity is concerned with preventing the loss of consumer's information. Due to the fact that clients often access data from the cloud service provider, this is quite crucial. Data integrity is attained through the following:

1.7.1. Verification Based on BLS Signature. A security method called the Boneh–Lynn–Shacham (BLS) signature is used to verify a signer's identity. This approach is built on the fundamentals of an elliptic curve and employs a bilinear pair for authentication. This increases its defenses against an index attack. This was used in the works of the authors in reference [36], who recognized the conventional flaws in privacy-preserving models' ability to guarantee data integrity. Key generation, token generation, challenge, response, and check proof are the five steps of verifiability in their approach. This strategy encourages auditing verification since it guarantees accurate verification.

1.7.2. Blockchain. Blockchain has been proposed as a cryptosystem alternative for protecting data integrity in the cloud. This is seen in the works of the authors in reference [37], where an integrated linear mapping technique was applied. As a result, third party auditors' trust issues are lessened while also saving significant computational and connection overheads. To create tags for the sample verification, the message is sliced and homomorphically verified.

1.8. Availability. Data availability guarantees that data stored in the cloud are accessible to its owners. This seeks to retrieve data in its entirety. The cloud client wants to ensure that none of the cloud service provider's internal data failures, device malfunctions, software defects, or other cloud dangers have had any impact on the data [38]. Replication of data is used nowadays to provide data availability, and the following setup by the cloud client automatically replicates data on two or more virtual servers. Amazon S3 and Google Cloud are the two well-known companies that provide multidata duplication at many locations [39].

1.9. Proposed Techniques Used to Secure the Cloud

1.9.1. Firewall. A firewall is implemented to guarantee protection against host and network threats. This makes it a useful security technique that may be applied to guarantee cloud security. The connection of devices can be evaluated and regulated by a firewall [40]. This aids in thwarting attacks such as cross-virtual machines (VM) and Economic Denial of Service (EDoS) [41]. Shielding internal nodes from outside threats aids in securing the entry of autonomous architecture and the system's security. Because cloud computing is dynamic, it might reduce the inner and outside security benefits that a firewall provides. Therefore, the external parties use rented instances to run their program [41]. This makes using firewall to be noted to maintain the privacy and security of cloud data quite safe.

1.9.2. Encryption. Data security in the cloud is achieved by using the right cryptographic technique. By using this method, the message is rendered unintelligible [42]. The encryption key used to carry out the encryption process determines how strong such methods are. Prime factorization, the foundation of an algorithm such as the RSA developed by Rivest, Shamir, and Adleman, is challenging to calculate in discrete logarithmic time. The cloud is protected by several cryptographic methods, including advanced encryption scheme (AES), DES, and Blowfish. Blowfish, AES, SHA1, and DES are just a few of the other integration techniques that are employed. All of them are used to guarantee cloud security. The most frequent attack on cryptography is thought to be a brute force attack.

1.9.3. Data Masking. Data masking is the ability to conceal genuine data from their natural structure while maintaining their authenticity to stop data leakage. This is viewed as

TABLE 2: Security challenges in cloud computing.

Cloud service	Security issues	Security challenges
Software as a service (SaaS)	(i) Malware attack (ii) Extensive data access (iii) Inadequate technical skills	(i) Visualizing data of users on the cloud (ii) Poor control of data in motion
Platform as a service (PaaS)	(i) Accessing the system by unapproved persons	(i) The problem with the unavailability of service (ii) Hijacking by attackers
Infrastructure as a service (IaaS)	(i) Security relating to virtualization (ii) Hardware security concerns (iii) Security issues relating to utility services	(i) Security issues relating to service level agreement (ii) Security of providing software using network
Container as a service (CaaS)	(i) The sharing of OS used by the host possess a security threat (ii) Security of apps in the container	(i) Critical concentration on run time is needed (ii) Securing container-to-container activities

a bridge connecting the token technique and encryption. By masking some parts of the message that consumers are not meant to view has the feature of hiding the actual data [43]. Based on legal restrictions, this method enables outsourcing, allocation, affiliation, and the use of cloud technologies.

Both types of dynamic and static data masking are taken into consideration. Dynamic masking is the use of selective concealment depending on legal considerations for data readers, providing security to sensitive data equivalent to plaintext without any scrambling properties. Data that have been hidden from view thanks to static data masking are irrevocable.

1.9.4. Blockchain (Distributed Ledger Technology). Blockchain is the ever-evolving technology that writers claim can potentially safeguard data in this era of information growth. The list of blocks is protected cryptographically since it is organized in hierarchical tiers. Using the connection of widely dispersed computers, their activities are organized in a peer style [44]. It prevents data loss, alteration, or manipulation by storing a duplicate of the mirrored data on each machine in the network. This contributes to improving the security of the data being managed.

Several studies, such as those conducted by the authors in references [45, 46], have attempted to address these security vulnerabilities. However, the present cryptographic techniques are incapable of withstanding contemporary security threats that target cloud customers and providers due to proportionality between data size and run time, making security a major setback to the full adoption of cloud computing. Again, as linear run times are produced as a result of the relationship between data size and run time, there is excessive CPU engagement creating wear and tear on client and provider equipment. Furthermore, such schemes require additional data transport bandwidth when large data are to be transferred [47].

As a result of the importance of securing data on the cloud, this paper conducts a systematic literature review of various published articles aimed at securing the cloud [48]. Also, this study unravels the type of cryptographic algorithms employed (symmetric, asymmetric, or protocol) [49] to attain cloud data security. Again, the trend of run times of these cryptographic algorithms (linear/nonlinear time), the purpose of these cryptographic algorithms, and cloud security concerns are also investigated by this study.

1.10. Identified Problem. Cloud computing is a growing and progressive technique to offer offshore storage and computing services that has become riskier in terms of security in recent years. The control and administration of an organization's data and assets are at the mercy of a third party, exposing the data to a variety of vulnerabilities such as confidentiality, privacy, data leakage, data theft, dependability, capacity, and performance assessment. As a result of these security difficulties, cryptographic approaches have been proposed by researchers as appropriate tools for ensuring the security of subscribers' data on the cloud. Despite the multiple cryptographic systems suggested

by experts, security remains a barrier to cloud computing's widespread adoption. Again, the run time and data sizes of these cryptographic systems are proportional, suggesting that the larger the data size, the longer the execution time, making the algorithm's execution times linear ($O(N)$). Because data volumes are related to execution time, when large amounts of data are outsourced to the cloud service provider, it puts wear and tear on both the cloud service provider and the cloud client devices. This has necessitated a review of published articles from 2016 to 2022 on the most commonly used cryptographic scheme to secure the cloud, the type of cryptographic algorithms used (symmetric, asymmetric, or protocol) to achieve cloud data security, the run times of these cryptographic algorithms (linear or nonlinear time), the purpose of these cryptographic algorithms, cloud security concerns, and cloud security techniques.

2. Literature Review

Researchers have paid close attention to cloud computing security. Several conferences, including the 2nd International Conference on Electrical, Communication, and Computer Engineering, the 2nd World Congress on Computing and Communication Technologies, and the ACM International Conference Proceeding Series (2020), have focused on cloud computing security. Aside from these, the majority of other publications have committed to publishing cloud computing-related papers aimed at accomplishing cloud security. This section discusses a thorough evaluation of works performed by researchers on cloud security.

The study of the authors in reference [50] looked at the Fusion-based Advanced Encryption Algorithm (FAEA) to offer a cost-effective, workable security architecture for using big data in the cloud. The performance of the FAEA approach was compared to that of the Map Reduce Encryption Scheme (MRE) and Hadoop Distributed File System (HDFS) and shows that it performed 98% better in terms of efficiency, scalability, and security.

In the work of the authors in reference [51], they challenged the attackers with more advanced security measures using a powerful real-time service-centric feature sensitivity analysis (RSFSA) model. The RSFSA model examines the sensitivity of various characteristics used by each service at several levels. The method computes the FLAG value for the user from the provided profile by checking the set of features being accessed at each level and the number of features to which the user has access permissions. The user has either been given access to the service or not, depending on FLAG's value. On the other hand, the technique maintains several encryption protocols and keys for every feature level. The technique maintains a set of schemes and keys for each level-specific feature since the features are grouped at different levels.

Muthulakshmi and Venkatesulu [52] proposed a revolutionary customized advanced encryption standard (AES) cryptographic algorithm. The goal of their technique is to improve the performance of the AES algorithm by

shortening the cryptography process. The notion of a chunk file system is proposed in an attempt to increase the efficiency of AES. The input file is chunked into numerous files, allowing for fast and efficient encryption. A comparative study is performed using the current algorithms' lightweight keyword searchable encryption (LFSE) and cloud key management system (CKMS) to demonstrate the effectiveness of their suggested system. The time required for key creation, encryption, and decryption is the basis for the comparative effort.

Rupa et al. [53] suggested a homomorphic encryption scheme based on matrix transformations using shifts, rotations, and transpositions of each letter in the plain text's binary transformed ASCII values. The symmetric cryptography uses the same secret key for both encryption and decoding.

William et al. [25] published a paper in which the researchers proposed combining symmetric and asymmetric methods, which are also processed by the hashing algorithm. The suggested approach first turns the provided data into cipher text using an AES algorithm with a key size of 128, 192, or 256 bits. The AES key is encrypted again using the Elliptical Curve Cryptography (ECC) technique. To construct the message digest, the encrypted text is again put through the Secure Hash Algorithm (SHA) 256 method. The encrypted message and the encrypted AES key are both transferred over the network, where the encrypted AES key is first decrypted using the ECC decryption technique, and then the AES decryption is performed using the retrieved key to recover the original plain text. The SHA digest is used to verify data integrity. The outcomes are computed for textual and picture datasets.

Data security in terms of attribute-based encryption, access control, and data integrity was evaluated by Rajeswari and Kalaiselvi in their study on cloud data storage [54]. Based on their findings, they concluded that the compute overhead for data storage and security should be reduced and that cloud security might be improved through verification, approval, privacy, and integrity.

El-Attar et al. [55] proposed a hybrid automated approach to preserve secrecy while achieving great efficiency during the encryption of huge data. The suggested technique comprises random key creation utilizing the RSA algorithm to generate private and encrypted keys. The data to be uploaded are separated into random-size blocks, and for each block, automated sequential cryptography and automated random cryptography are used. The encrypted blocks are then saved in the cloud. Both sequential and random algorithms rely heavily on AES and DES methods. Both automated systems achieved a high degree of security as well as great efficiency during encryption and decryption. The findings are also compared with better automated random cryptography based on the S-Box generator. When compared to the prior approaches, this new algorithm produced more efficient outcomes.

Data security was improved by Mani and Devi [56] by using preprocessing before encryption. The first level of security is achieved by encoding the provided plain text using the Lucas and Fibonacci series. The second level of

security is then achieved by further compressing the encoded text using the Huffman encoding, and the third level of security is attained by subjecting it to the RSA public key cryptographic algorithm. In the reverse process, the encrypted text is transformed back to the original plain text by being first decrypted, then decompressed, and lastly decoded.

Khalid Yousif et al. [57] used the (NTRUEncrypt) algorithms in Hadoop to speed up the file encryption and decryption procedures in their investigation. If HDFS is involved in the Map Task, it will handle both the encryption and decryption procedures. The suggested protection approach, which employs cryptography, can keep data on the cloud private and safe.

Yang et al. [58] proposed a novel cloud-based parallel block Wiedemann technique for solving large and sparse linear problems over GF (2). Strip partitioning, cyclic partitioning, and modified strip partitioning are included in the proposed parallel block Wiedemann method to parallelize distinct phases in the block Wiedemann process.

Through the fusion of two approaches, Kumar [59] devised a cryptographic algorithm to attain security of cloud data. These two supplied a significantly more secure data security platform, namely, the DNA-based algorithm and the AES algorithm. Data encryption and decryption are performed using the DNA cryptographic technology and the AES method. DNA encryption enables you to encrypt a lot of data with only a small bit of DNA.

In the research study of Suganya and Sasipraba [60], a genetic crossover-based cryptography system was proposed. This was a unique encryption technique used to store sensitive and nonsensitive data in a heterogeneous multi-cloud environment in order to guard against the riskiest activities, such as data breaches, man-in-the-middle attacks, and insider attacks. To increase the security of the data, the file was encrypted using the suggested prime crossover approach and stored in several cloud settings. Data integrity, confidentiality, and accessibility are not compromised in this way.

Aruna and Mohan [40] developed an efficient probabilistic public key eEncryption (EPPKE) as a cryptographic method to protect data in the cloud. Covariance Matrix Adaptation Evolution Strategies (CMA-ESs) are used to optimize this strategy. By using the Luhn algorithm and BLAKE 2b encapsulation, it guarantees data integrity. This allows enhanced protection for data that are sent over the cloud.

According to the previous studies, the use of cryptographic algorithms is the primary emphasis when it comes to guaranteeing data security in the cloud. However, little has been said about the most commonly used cryptographic approach for securing data in the cloud, the type of cryptographic algorithms used (symmetric, asymmetric, or protocol), the trend of the cryptographic algorithm run times (linear or nonlinear time), the purpose of these cryptographic algorithms, and cloud security concerns. Again, none of the materials available are from African academics, showing that there is a big gap in Africa when it comes to security issues in cloud applications.

3. Methodology

The number of works regarding cloud data security is taken into account in this study and their interpretation is based on publications on the subject, and a systematic literature evaluation based on PRISMA is produced.

3.1. Research Questions. The goal of this study is to assess the security concerns with cloud computing. Researchers' security interventions are also taken into account. This study takes six objectives into account. These goals are as follows:

What is the most often used cryptographic technique for cloud data security?

Which type of cryptographic algorithms is used to secure data on the cloud?

How can cryptographic algorithms encrypt and decrypt cloud data?

In terms of linear versus nonlinear time, what is the trend in the execution time of the used cryptographic algorithms?

What are the intended aims of these cryptographic schemes?

What are some of the security concerns in cloud computing?

3.2. Approaches for Accessing Articles. This section focuses on the different terms, databases, reference tools, and search methods used in answering the research questions. This has been well discussed as follows.

3.3. Phrases Used. To arrive at the various articles utilized in this study, several keyword searching was employed such as "Data security in the cloud," "Cloud security challenges," "Cloud security models," "Cloud providers and security challenges," and "Cloud security mitigation strategies."

3.3.1. Electronic Sources. Several well-known digital resources were utilized to find publications for this study, including Taylor & Francis, Scopus, Research Gate, Web of Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, Emerald, Sage, Wiley online library, and ACM.

3.3.2. Reference Management. Based on the search terms, a considerable number of articles were downloaded. The IEEE reference creation tool was utilized as the referencing management tool.

3.3.3. Search Processes. The popular databases were searched to obtain articles related to the subject at hand. This included journal papers, conference proceedings, and books. All 157 papers were downloaded, and they were arranged for reading and referencing convenience using an IEEE reference generator and Mendeley. The results are then shown in a PRISMA framework as shown in Figure 4

[61]. The publications were grouped using a selection technique based on their relevance using their center of interest, and 72 of the 157 publications were deemed relevant to the issue under consideration. The exclusion procedure used for the selection of the papers of interest is as follows:

- (I) Papers with publication dates earlier than 2015
- (II) Papers with no DOI
- (III) Papers with a concentration on cloud taxonomy
- (IV) Articles using anonymous citation
- (V) Papers that concentrate on technology other than cloud computing security.

4. Results

The results of the systematic literature review are presented in this part, and their commentary is provided in the supplemental subsections. Table 3 categorizes the list of publications, the purpose of the algorithm, the number of sources and references, and the run time trend of these cryptographic algorithms. The table provides clear guidelines for academics looking for answers to cloud security issues. There is also the concern that, despite the benefits of cloud computing, cloud clients are unwilling to shift to the cloud.

4.1. What Is the Most Often Used Cryptographic Technique for Cloud Data Security? According to Figure 5 and Table 3, the adoption of encryption techniques, which accounts for 16.7% of publications from 2017 to 2021, is the most popular method for ensuring cloud security. The existing cryptographic techniques and hybrid algorithms were utilized in these encryption schemes. This was followed by the usage of encryption models, which represented 9.7% of the total. The most often used encryption approach was based on the MapReduce layer, which was implemented on a Hadoop platform [62].

4.2. Which Type of Cryptographic Algorithms Are Used to Secure Data on the Cloud? The many cryptographic algorithms used to safeguard data in the cloud are depicted in Figure 6. These are divided into two types, namely, asymmetric and symmetric algorithms. Figure 6 shows that, in 2016, 2% of the published papers utilized in this review were based on both symmetric and asymmetric features. This threshold was raised to 5% for asymmetric algorithms and 4% for symmetric algorithms. In 2021, there was considerable growth in the adoption of asymmetric methods to protect data in the cloud, with a proportion of 8% vs. 7% for symmetric algorithms. Asymmetric algorithms fell from 8% in 2021 to 0% in 2022, and symmetric algorithms fell from 7% in 2021 to 1% in 2022.

4.3. How Can Cryptographic Algorithms Encrypt and Decrypt Cloud Data? On the cloud, data encryption and decryption are accomplished in two ways. The first method is to encrypt

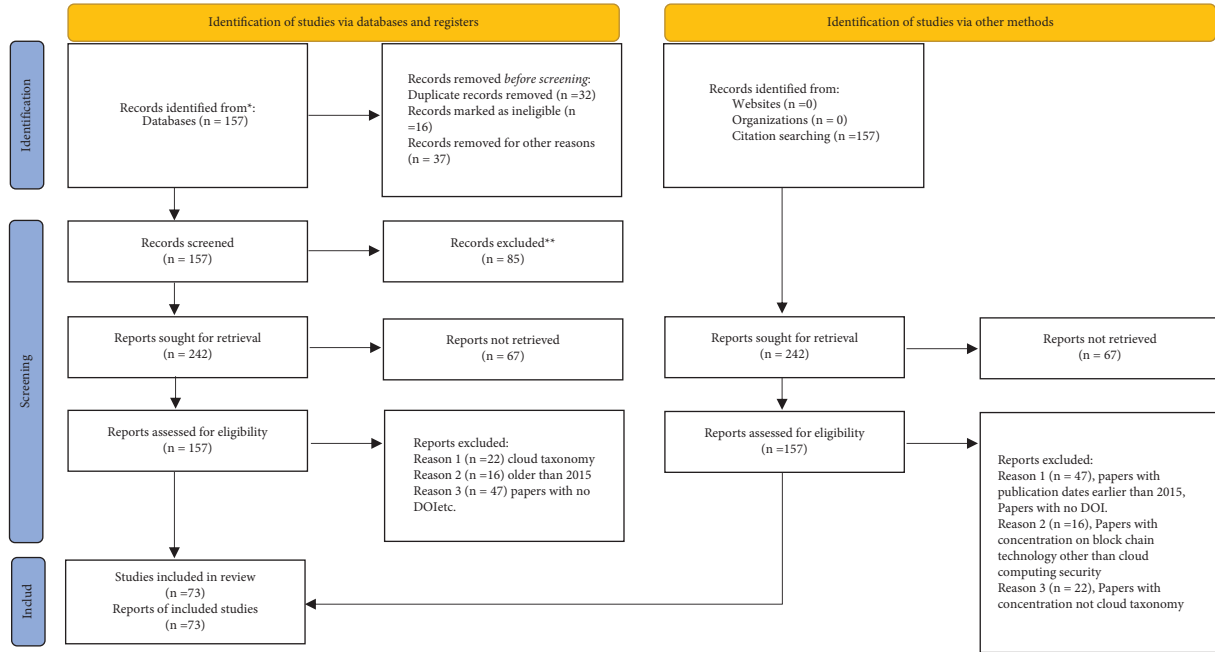


FIGURE 4: Flow diagram for the systematic review which included searches of databases and other sources [61].

TABLE 3: Papers used in the survey.

Purpose of the algorithm	Number of sources and references	Run time trend
Data security	24 (64, 68, 70, 71, 78, 80, 81, 82, 83, 84, 86, 87, 88, 89, 90, 112, 116, 118, 119, 120, 121, 123, 130, 134)	Linear
Attack on cloud	1 (65)	Linear
Privacy and preservation	1 (66)	Linear
Security analysis	1 (67)	Linear
Data protection	1 (69)	Linear
Cloud security	34 (72, 73, 74, 76, 77, 79, 91, 93, 94, 95, 96, 97, 98, 100, 101, 102, 103, 104, 105, 108, 110, 111, 113, 114, 115, 117, 122, 124, 125, 128, 129, 133, 135, 136)	Linear
Intrusion detection	1 (75)	Linear
Security, privacy and trust	1 (85)	Linear
Security and privacy	5 (92, 99, 107, 126, 131, 132)	Linear
Data privacy	1 (106)	Linear
Security and privacy	2 (109, 127)	Linear

the entire data as a block, which is known as block ciphering, while the second method is to execute the data alphabet by alphabet, which is known as stream ciphering. According to Figure 7, 4% of the algorithms proposed in 2016 utilized a block cipher method, whereas 0% used a stream cipher strategy. However, the use of block cipher algorithms increased to 10% in 2020, with a comparable 2% for stream cipher methods. The use of block cipher algorithms fell from 10% in 2020 to 9% in 2021, while stream cipher algorithms increased by 7% in 2021.

4.4. In Terms of Linear versus Nonlinear Time, What Is the Trend in the Execution Time of the Used Cryptographic Algorithms? The execution time trend evaluates an algorithm's performance by measuring how long it takes to encrypt and decrypt data of various sizes [62]. The

execution time of an algorithm is classified as linear or nonlinear according to its performance evaluation. Linear performance evaluation is noticed when the algorithm's execution time is proportionate to the data size ($O(N)$). As a result, the larger the data amount, the longer the execution time, as demonstrated by the works of the authors in reference [63]. However, the efficiency of the nonlinear method is determined not by data quantity but by the magnitude of the nonce value employed during algorithm execution [64].

According to Figure 8, linear and nonlinear algorithms were used 1% of the time in 2016. The use of linear algorithms increased by 12% in 2020, representing an 11% rise over the period of 2016, with no interest in nonlinear algorithms remaining at 0%. In 2021, researchers focused heavily on linear algorithms, resulting in 14%, with nonlinear execution time techniques remaining at 0%.

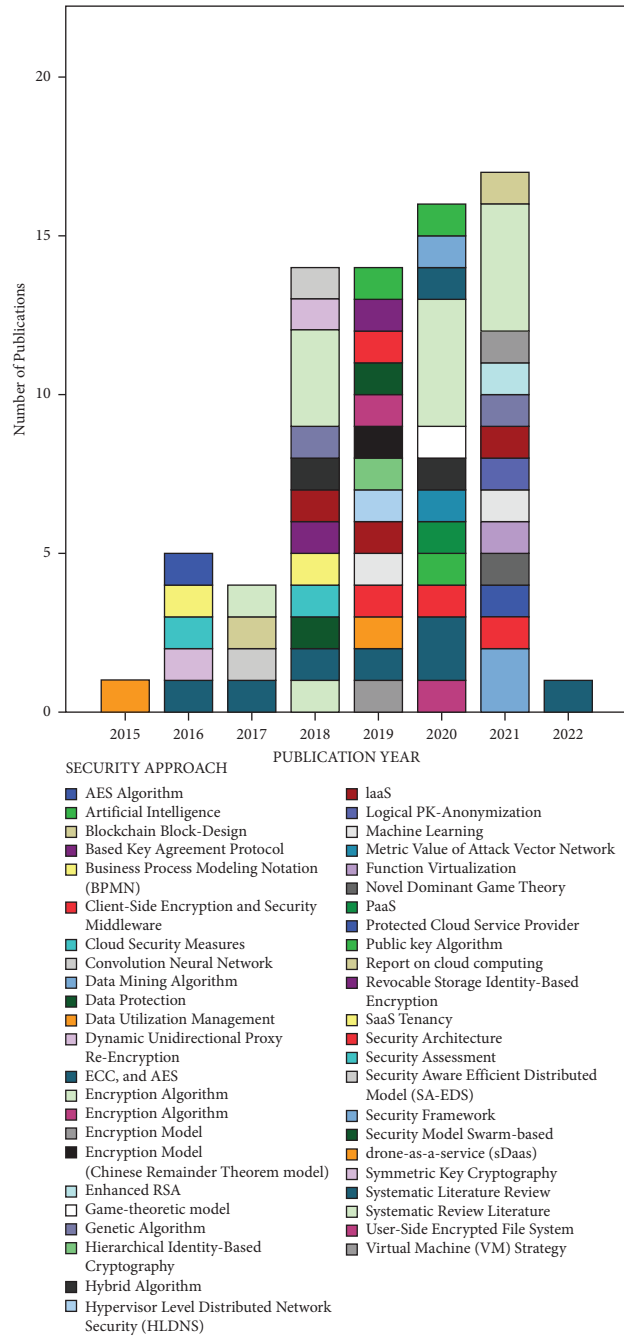


FIGURE 5: The most employed cryptographic scheme used to secure data on the cloud.

4.5. *What Are the Intended Aims of These Cryptographic Schemes?* The different goals for using the different cryptographic techniques are shown in Figure 9. Cryptographic techniques are procedures used to handle cloud security concerns such as data privacy, cloud security, data confidentiality, and data security. According to Figure 9 and Table 3, guaranteeing data security on the cloud accounts for 30.6% of all articles included in this survey from 2016 to 2022. This is obvious in the works of the authors in

references [50, 52–56, 58, 65] and [66, 67] where data security has been the primary priority.

Cloud security was next, accounting for 29.2% of all publications included in this systematic literature review backed by the work of the authors in reference [40]. Figure 9 and Table 3 show that just 2% of publications focused on data confidentiality, as suggested by the author in reference [59] in related works. The procedures used are mostly for cloud penetration testing and anomaly detection.

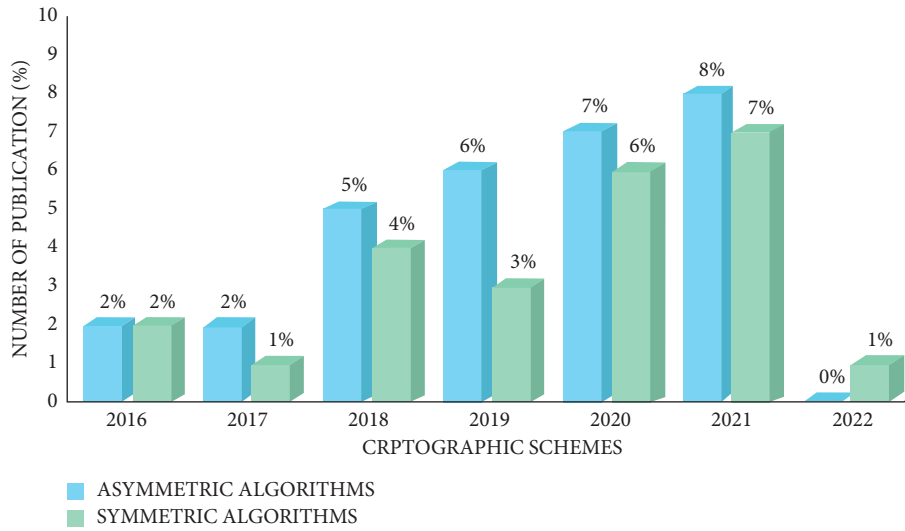


FIGURE 6: Type of cryptographic algorithms used to secure data on the cloud.

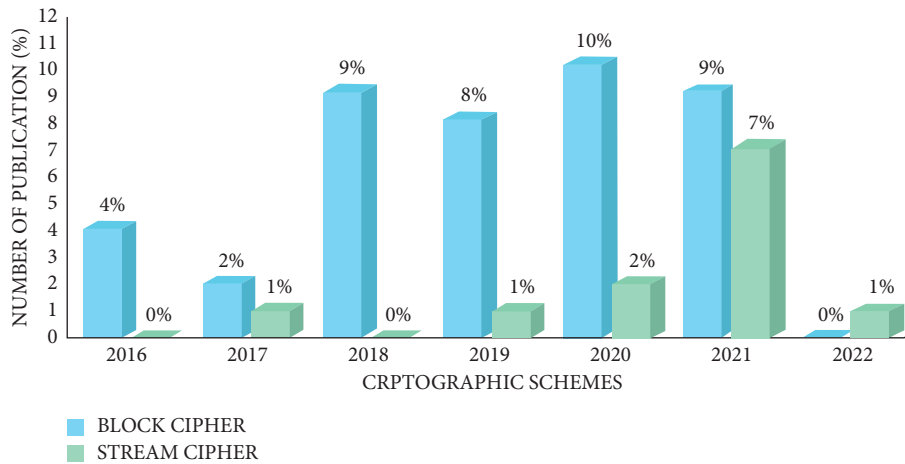


FIGURE 7: How cryptographic schemes encrypt and decrypt data on the cloud.



FIGURE 8: Execution time trend of cryptographic algorithms used to secure data on the cloud.

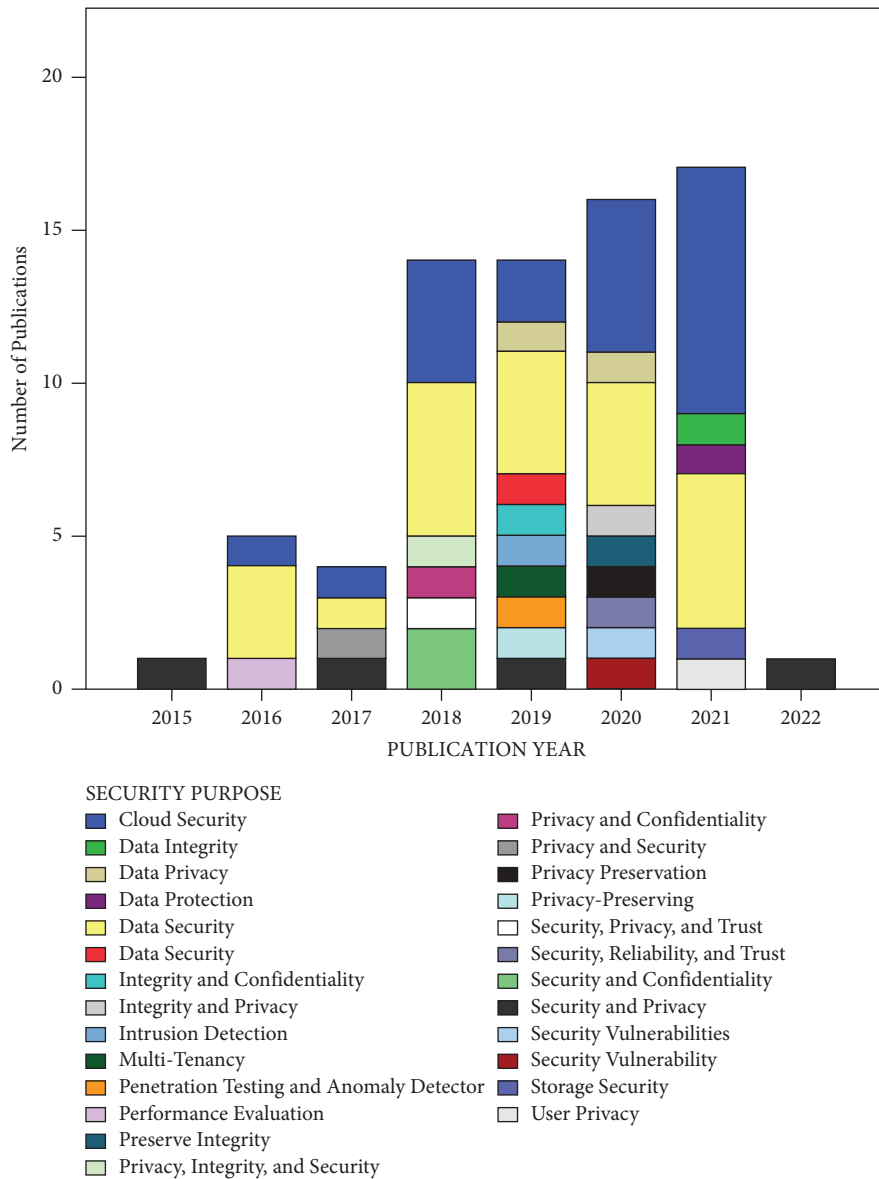


FIGURE 9: Intended aims of cryptographic schemes.

4.6. *What Are Some of the Security Concerns in Cloud Computing?* Aside from the benefits of cloud computing, cloud clients and cloud service providers present several concerns. As a result, they are unable to fully transition to the cloud [68]. This is obvious in Gartner’s categorization of cloud security risk, which is divided into seven segments [69]. Gartner’s security concerns are classified into the following seven categories:

- (I) *Access Control.* This manages the inflow and outflow of access to data by cloud clients
- (II) *Governance.* This controls clients’ data security and integrity
- (III) *The geographical location of data.* This controls the siting of data centers to store clients’ data

- (IV) *Division of data.* This defines the ways to break data into units for storage.
- (V) *Data Recovery.* The ability to recover data in case of a disaster such as a virus attack
- (VI) *Fact-finding.* This explains if there is the possibility to investigate any illicit task
- (VII) *Data Availability.* This is to find out if the stored data will be made available anytime they are needed by the cloud client.

These seven categorizations of Gartner’s category have led to the security challenges depicted in Figure 10.

Table 3 depicts the various publications which were surveyed from renowned digital data sources such as Taylor and Francis, Scopus, Research Gate, Web of

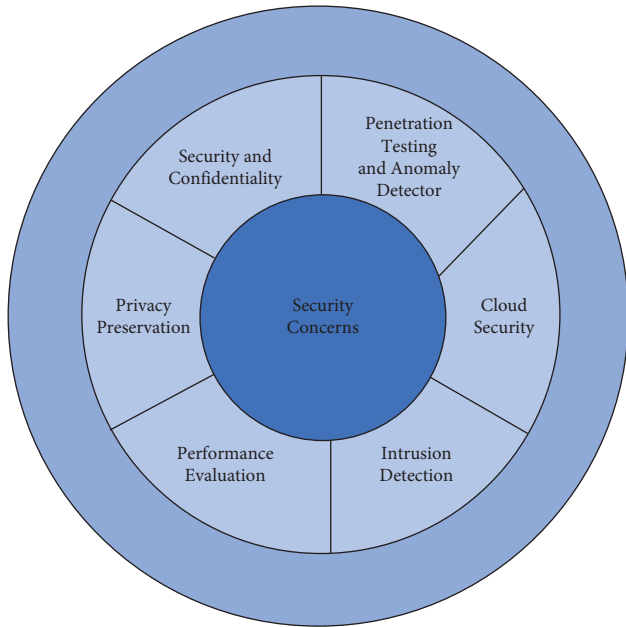


FIGURE 10: Security concerns in the cloud.

Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, and ACM.

A thorough analysis of the articles from well-known databases has indicated that many researchers have put in the effort to safeguard the cloud as shown in Table 3. From Table 3, it is evident that 46.58% of the articles used in this study were all directed towards achieving cloud security. Also, 24 of the articles aimed at ensuring data security in the cloud, representing 32.88% of the articles used in this study. This indicates that excessive work has been performed concerning the cloud security. However, from Table 3, it is evident that all of the algorithms' run-time trends are linear ($O(N)$). This implies that run times and data sizes are proportionally related. This results in excessive engagement of the CPU when large data sizes are executed which cause wear and tear of gadgets. This makes algorithms executions time predictable and gives room for hackers to hack systems because of prejudice of the run time. The linear nature of the proposed algorithms results in higher execution times. Again, except for algorithms that employ hash functions, linear run-time algorithms require significant bandwidth to transfer data to the cloud due to the growth in data volumes resulting from data size and run-time relationships. This is a major weakness of the majority of proposed algorithms directed towards securing the cloud.

5. Limitations

This comprehensive review of the literature covers various articles that explore the study's objectives. The authors are confident that this systematic literature review will cover the type of cryptographic algorithms used (symmetric, asymmetric, or protocol), the trend of run times for these cryptographic algorithms (linear/nonlinear time), the purpose of these cryptographic algorithms, and cloud security concerns published between 2016 and 2022. One of the

limitations of this SLR is the use of simple search terms to discover research papers. Such search terms, on the other hand, can be broadened. Again, publications that did not have a digital object identifier (DOI) and were not deemed relevant papers limit our analysis. Another shortcoming of this SLR is that it excludes very recently published research articles that should have been included in this SLR to address the research questions.

6. Conclusion

A systematic literature review approach was used in this study to review the literature on cloud computing, with a focus on the most commonly used security approach to control security issues in the cloud, the type of encryption algorithms used to secure the cloud, how algorithms encrypt and decrypt data on the cloud, the run-time trends of the algorithms used in the cloud (linear time/nonlinear time), and the intended aims of these security approaches. Many security methods, such as firewalls, data masking, encryption, and blockchain, have been identified as answers to data security concerns.

The recognized security challenges included confidentiality and privacy, which may be achieved through encryption. Data integrity as a security concern may be achieved using BLS signature verification and blockchain. Data availability has also been noted as a security risk in cloud computing, which may be solved by data replication across several servers. The cloud migration has the advantages for cloud customers and cloud service providers, but maximizing these profits needs effective and long-term security measures to address the breach of security problems in cloud computing. This comprehensive literature study highlighted security as a key barrier to complete cloud computing adoption on the side of both the cloud customer and the cloud service provider. Furthermore, the comprehensive literature analysis revealed that encryption techniques are the best ways to secure the cloud. The paper states that linear time complexity algorithms account for 90% of the encryption algorithms proposed from 2016 to 2022, making linear ($O(N)$) time algorithms the most popular and widely used.

However, the present cryptographic techniques are incapable of withstanding contemporary security threats that target cloud customers and providers face due to their linear run times. Because linear run times are dependent on data size, attackers may estimate the time required for each data execution. Furthermore, such encryption techniques need additional data transport bandwidth when large data are to be transferred [47]. When huge volumes of data are sent, the reliance on data proportionality and run times creates wear and tear on the client's and provider's equipment.

7. Recommendation

- (i) Cloud service providers should use nonlinear algorithms as security schemes to ensure the interoperability of devices with lesser specifications.
- (ii) Stakeholders in device developing and manufacturing should consider using nonlinear algorithms to ensure security of data on their devices.

8. Future Works

- (i) There is limited literature on nonlinear algorithms to secure data on the cloud; as a result, more research should be conducted on nonlinear algorithms ($f(x) = b - cx^2$).
- (ii) More studies should be conducted on cloud challenges such as confidentiality and privacy, multi-tenancy, and data reliability.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] I. Ibrahim and M. Bassiouni, "Improvement of job completion time in data-intensive cloud computing applications," *Journal of Cloud Computing*, vol. 9, no. 1, 2020.
- [2] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: a survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020.
- [3] A. Markandey, P. Dhamdher, and Y. Gajmal, "Data access security in cloud computing: a review," in *Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 633–636, Greater Noida, India, September 2018.
- [4] M. O. Alassafi, R. AlGhamdi, A. Alshdadi, A. Al Abdulwahid, and S. T. Bakhsh, "Determining factors pertaining to cloud security adoption framework in government organizations: an exploratory study," *IEEE Access*, vol. 7, pp. 136822–136835, 2019.
- [5] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine learning for cloud security: a systematic review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021.
- [6] F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. Kent, and S. Hakak, "Cloud computing security: a survey of service-based models," *Computers and Security*, vol. 114, Article ID 102580, 2022.
- [7] N. Alkhater, R. Walters, and G. Wills, "An empirical study of factors influencing cloud adoption among private sector organisations," *Telematics and Informatics*, vol. 35, no. 1, pp. 38–54, 2018.
- [8] O. Alfandi, H. Said, and S. Khanji, *Analysis of Cloud Computing Attacks and Countermeasures*, Academia.edu, San Francisco, CA, USA, 2022.
- [9] S. Liu, K. Yue, H. Yang, L. Liu, X. Duan, and T. Guo, "The research on SaaS model based on cloud computing," in *Proceedings of the 2018 2nd IEEE Advanced Information Management, Communicates, Electronic, and Automation Control Conference (IMCEC)*, pp. 1959–1962, Xi'an, China, May 2018.
- [10] M. Saraswat and R. C. Tripathi, "Cloud computing: analysis of top 5 CSPs in SaaS, PaaS, and IaaS platforms," in *Proceedings of the 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pp. 300–305, Moradabad, India, December 2020.
- [11] S. Y. Abdel Ghany and H. Mamdouh Hassan, "Get as you pay model for IaaS cloud computing," in *Proceedings of the 2018 International Conference on Smart Communications and Networking (SmartNets)*, pp. 1–6, Yasmine Hammamet, Tunisia, November 2018.
- [12] M. Hussein, M. Mousa, and M. Alqarni, "A placement architecture for a container as a service (CaaS) in a cloud environment," *Journal of Cloud Computing*, vol. 8, no. 1, 2019.
- [13] C. Li and C. Yang, "A novice group sharing method for public cloud," in *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, July 2018.
- [14] W. Hassan, T.-S. Chou, L. Pagliari, J. Pickar, and O. Tamer, "Is public cloud computing. A. Patel," "A survey on security techniques used for confidentiality in cloud computing," in *Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, pp. 1–6, Kottayam, India, December 2018.
- [15] M. Tajammul and R. Parveen, "To carve out private cloud with total functionality," in *Proceedings of the 2020 2nd International Conference on Advances in Computing Communication Control and Networking (ICACCCN)*, pp. 831–835, Greater Noida, India, December 2020.
- [16] S. Yi, L. Yuhe, and W. Yu, "Cloud computing architecture design of database resource pool based on cloud computing," in *Proceedings of the 2018 International Conference on Information Systems and Computer Aided Education (ICISCAE)*, pp. 180–183, Changchun, China, July 2018.
- [17] S. Sok, C. Plewnia, S. Tanachutiwat, and H. Lichter, "Optimization of compute costs in hybrid clouds with full rescheduling," in *Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 35–40, Washington, DC, USA, November 2020.
- [18] D. S. Linthicum, "Emerging hybrid cloud patterns," *IEEE Cloud Computing*, vol. 3, no. 1, pp. 88–91, 2016.
- [19] R. Baig, F. Freitag, and L. Navarro, "Cloudy in guifi.net: establishing and sustaining a community cloud as open commons," *Future Generation Computer Systems*, vol. 87, pp. 868–887, 2018.
- [20] K. Dubey, M. Y. Shams, S. C. Sharma, A. Alarifi, M. Amoon, and A. A. Nasr, "A management system for servicing multi-organizations on community cloud model in secure cloud environment," *IEEE Access*, vol. 7, pp. 159535–159546, 2019.
- [21] S. Bruque-Cámara, J. Moyano-Fuentes an, and D. J. Maqueira-Marín, "Supply chain integration through community cloud: effects on operational performance," *Journal of Purchasing and Supply Management*, vol. 22, no. 2, pp. 141–153, 2016.
- [22] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The Journal of Supercomputing*, pp. 9493–9532, 2020.
- [23] S. Singh, Y. Jeong, and J. Park, "A survey on cloud computing security: issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.
- [24] D. Malviya and U. Lillhore, "Survey on security threats in cloud computing," *International Journal of Trend in Scientific Research and Development*, vol. 3, no. -1, pp. 1222–1226, 2018.
- [25] P. William, A. Choubey, G. S. Chhabra, R. Bhattacharya, K. Vengatesan, and S. Choubey, "Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content," in *Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pp. 918–922, Tuticorin, India, March 2022.
- [26] M. Joshi, S. Budhani, N. Tewari, and S. Prakash, "Analytical review of data security in cloud computing," in *Proceedings of the 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 362–366, London, UK, April 2021.

- [27] W. Isharufe, F. Jaafar, and S. Butakov, "Study of security issues in platform-as-a-service (PaaS) cloud model," in *Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pp. 1–6, Istanbul, Turkey, June 2020.
- [28] A. Gupta and S. Gupta, "Security issues in big data with cloud computing," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 5, no. 6, pp. 27–32, 2017.
- [29] I. K. Sahu and M. J. Nene, "Model for IaaS security model: MISP framework," in *Proceedings of the 2021 International Conference on Intelligent Technologies (CONIT)*, pp. 1–6, Hubli, India, June 2021.
- [30] S. Sultan, I. Ahmad, and T. Dimitriou, "Container security: issues, challenges, and the road ahead," *IEEE Access*, vol. 7, pp. 52976–52996, 2019.
- [31] K. Timraz, T. Barhoom, and T. Fatayer, "A confidentiality scheme for storing encrypted data through cloud," in *Proceedings of the 2019 IEEE 7th Palestinian International Conference on Electrical and Computer Engineering (PICECE)*, pp. 1–5, Gaza, Palestine, March 2019.
- [32] R. Ma, J. Li, H. Guan, M. Xia, and X. Liu, "EnDAS: efficient encrypted data search as a mobile cloud service," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 3, pp. 372–383, 2015.
- [33] N. A. Patel, "A survey on security techniques used for confidentiality in cloud computing," in *Proceedings of the 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, pp. 1–6, Kottayam, India, December 2018.
- [34] K. Cheng, "Secure \$k\$-NN query on encrypted cloud data with multiple keys," *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 689–702, 2021.
- [35] S. Gokulakrishnan and J. M. Gnanasekar, "Data integrity and Recovery management in cloud systems," in *Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, pp. 645–648, Coimbatore, India, January 2020.
- [36] X. Luo, Z. Zhou, L. Zhong, J. Mao, and C. Chen, "An effective integrity verification scheme of cloud data based on bls signature," *Security and Communication Networks*, vol. 2018, Article ID 2615249, 11 pages, 2018.
- [37] H. Wang and J. Zhang, "Based data integrity verification for large-scale IoT data," *IEEE Access*, vol. 7, pp. 164996–165006, 2019.
- [38] A. Juels and A. Oprea, "New approaches to security and availability for cloud data," *Communications of the ACM*, vol. 56, no. 2, p. 64, 2013.
- [39] S. Kang, B. Veeravalli, K. M. Mi Aung, and C. Jin, "An efficient scheme to ensure data availability for a cloud service provider," in *Proceedings of the 2014 IEEE International Conference on Big Data (Big Data)*, pp. 15–20, Washington, DC, USA, October 2014.
- [40] M. G. Aruna and K. G. Mohan, "Secured cloud data migration technique by competent probabilistic public key encryption," *China Communications*, vol. 17, no. 5, pp. 168–190, 2020.
- [41] J. Li, H. Jiang, W. Jiang, J. Wu, and W. Du, "SDN-Based stateful firewall for cloud," in *Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 157–161, Baltimore, MD, USA, May 2020.
- [42] R. H. Joshi, D. P. Rathi, A. Khan, and M. Jain, "A survey on various security issues and challenges to secure cloud computing," *International Journal of Innovative Research in Computer Science and Technology*, vol. 6, no. 3, pp. 31–35, 2018.
- [43] S. Mansfield-Devine, "Masking sensitive data," *Network Security*, vol. 2014, no. 10, pp. 17–20, 2014.
- [44] S. Uthayashangar, T. Dhanya, S. Dharshini, and R. Gayathri, "Decentralized-based system for secure data storage in cloud," in *Proceedings of the 2021 International Conference on System, Computation, Automation, and Networking (ICSCAN)*, pp. 1–5, Puducherry, India, July 2021.
- [45] P. T. Dinh and M. Park, "Dynamic economic-denial-of-sustainability (DDoS) detection in SDN-based cloud," in *Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 62–69, Paris, France, April 2020.
- [46] N. Saravanan and A. Umamakeswari, "Lattice-based access control for protecting user data in cloud environments with hybrid security," *Computers & Security*, vol. 100, Article ID 102074, 2021.
- [47] A. Q. Khan, "Smart data placement using storage-as-a-service model for big data pipelines," *Sensors*, vol. 23, no. 2, p. 564, 2023.
- [48] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, "A secure cloud computing system by using encryption and access control model," *Journal of Information Processing Systems*, vol. 15, no. 3, pp. 538–549, 2019.
- [49] R. B. Marqas, S. M. Almufti, and R. R. Ihsan, "Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms," *Xi'an Jianzhu Keji Daxue Xuebao/Journal of Xi'an University of Architecture and Technology*, vol. 12, no. 3, pp. 3110–3116, 2020.
- [50] A. Vidhya and P. M. Kumar, "Fusion-based advanced encryption algorithm for enhancing the security of big data in cloud," *Concurrent Engineering*, vol. 30, 2022.
- [51] A. Siva Kumar, S. Godfrey Winster, and R. Ramesh, "Efficient sensitivity orient blockchain encryption for improved data security in cloud," *Concurrent Engineering*, vol. 29, 2021.
- [52] B. Muthulakshmi and M. Venkatesulu, "A novel security mechanism using AES cryptography approach in cloud computing," *International Journal of Communication Systems*, vol. 34, no. 6, 2021.
- [53] C. Rupa, Greeshmanth, and M. A. Shah, "Novel secure data protection scheme using Martino homomorphic encryption," *Journal of Cloud Computing*, vol. 12, no. 1, 2023.
- [54] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," in *Proceedings of the 2017 IEEE International Conference on Circuits and Systems (ICCS)*, pp. 76–81, Thiruvananthapuram, Kerala, India, December 2017.
- [55] N. E. El-Attar, D. S. El-Morshedy, and W. A. Awad, "A new hybrid automated security framework to cloud storage system," *Cryptography*, vol. 5, p. 4, 2021.
- [56] K. Mani and A. Devi, "Enhancing security in cryptographic algorithm based on LECCRS," *Electronic Government, an International Journal*, vol. 13, no. 1, p. 31, 2017.
- [57] M. Khalid Yousif, Z. E. Dallalbashi, and S. W. Kareem, "Information security for big data using the NTRUEncrypt method," *Measurement: Sensors*, vol. 27, Article ID 100738, 2023.
- [58] L. T. Yang, G. Huang, J. Feng, and L. Xu, "Parallel GNFS algorithm integrated with parallel block Wiedemann

- algorithm for RSA security in cloud computing,” *Information Sciences*, vol. 387, pp. 254–265, 2017.
- [59] A. Kumar, “Data security and privacy using dna cryptography and aes method in cloud computing,” in *Proceedings of the 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, November 2021.
- [60] M. Suganya and T. Sasipraba, “Security and privacy-efficient encryption algorithm for cloud data using genetic prime crossover technique,” in *Proceedings of the 2022 1st International Conference on Computational Science and Technology (ICCSST)*, Chennai, India, November 2022.
- [61] M. J. Page, “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” *BMJ*, vol. 372, no. 71, p. n71, 2021.
- [62] M. La Manna, L. Treccozi, P. Perazzo, S. Saponara, and G. Dini, “Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update,” *Sensors*, vol. 21, no. 2, p. 515, 2021.
- [63] G. C. C. F. Pereira, R. C. A. Alves, F. L. da Silva, R. M. Azevedo, B. C. Albertini, and C. B. Margi, “Performance evaluation of cryptographic algorithms over iot platforms and operating systems,” *Security and Communication Networks*, vol. 2017, Article ID 2046735, 16 pages, 2017.
- [64] R. Masram, V. Shahare, J. Abraham, and R. Moona, “Analysis and comparison of symmetric key cryptographic algorithms based on various file features,” *International journal of Network Security and Its Applications*, vol. 6, no. 4, pp. 43–52, 2014.
- [65] G. Farid, N. F. Warraich, and S. Iftikhar, “Digital information security management policy in academic libraries: a systematic review (2010–2022),” *Journal of Information Science*, vol. 1, 2023.
- [66] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A systematic literature review on cloud computing security: threats and mitigation strategies,” *IEEE Access*, vol. 9, p. 1, 2021.
- [67] D. Ahamad, S. Alam Hameed, and M. Akhtar, “A multi-objective privacy preservation model for cloud security using hybrid jaya-based shark smell optimization,” *Journal of King Saud University- Computer and Information Sciences*, vol. 34, 2020.
- [68] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring data security issues and slutions in cloud computing,” *Procedia Computer Science*, vol. 125, pp. 691–697, 2018.
- [69] M. Ahmed and A. T. Litchfield, “Taxonomy for identification of security issues in cloud computing environments,” *Journal of Computer Information Systems*, vol. 58, no. 1, pp. 79–88, 2016.