Journal of Theoretical and Applied Information Technology
31st March 2023. Vol.101. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RECONNOITERING SECURITY ALGORITHMS PERFORMANCE IN THE CLOUD: SYSTEMATIC LITERATURE REVIEW BASED ON THE PRISMA ARCHETYPE

JOHN KWAO DAWSON[1*], DR. TWUM FRIMPONG[2], PROF. JAMES BENJAMIN HAYFRON ACQUAH[3], DR. YAW MARFO MISSAH[4]

Department of Computer Science, Sunyani Technical University, Ghana[1]
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana [2]
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana[3]
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana[4]

E-mail: [1]Kwaodawson1@yahoo.com, [2]twumf@yahoo.co.uk, [3]jbha@haoo.com, [4]ymissah@gmail.com

ABSTRACT

Industries and academia have embraced cloud computing for their day-to-day activities. A lot of studies have been done to unpin variants of cryptographic algorithms used to secure the cloud. This survey aims to unravel recent studies of the most employed cryptographic scheme used to secure the cloud, the type of cryptographic algorithms used, the execution time trend of the cryptographic algorithms (Linear time / Non-Linear time), the aims of these cryptographic algorithms, and identify some of the security concerns in cloud computing. The study considered published studies from 2015 to 2022 from well-known databases such as Taylor and Francis, Scopus, Research Gate, Web of Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, and ACM. A total of 72 published articles were considered to respond to the various specific objectives using the Prisma framework. The systematic literature review has revealed the usage of encryption schemes as the most employed cryptographic approach and data security and cloud security as the most researched security challenge. The security challenges that were identified are data integrity and preservation, intrusion detection, and privacy and confidentiality. It has been revealed that from 2015 to 2022, 90% of encryption algorithms depict linear time complexity. The systematic literature review has proven little usage of symmetric stream cipher algorithms to ensure the privacy and confidentiality of cloud data.
Keywords: *Data Security, Data Confidentiality, Data Integrity, Linear, Non-Linear, Intrusion Detection*

1. INTRODUCTION

There are a lot of challenges and opportunities recently as data production and usage have increased significantly in the world. In an attempt by data security experts to protect this huge data, a paradigm shift in data storage, security, integrity, and availability needs to be employed [1]. The remedy to these problems is through the adoption of cloud computing. The rendering of computing services hosted over the internet based on subscription is considered cloud computing [2]. Cloud computing usage allows for the employment of software and infrastructure in any place on this earth, where all the services are managed by cloud service providers [3]. It has been on the agenda of companies and governments around the world to adopt cloud computing to attain reduced operation cost and elasticity of data capabilities, which is assumed to be the best Information Technology solution [4]. The adoption of the cloud by governments and companies has resulted in various service providers springing up and notably among them are Salesforce, Amazon, and Yahoo with many vendors like IBM and Oracle that provide database technical support [5].

Despite the numerous benefits and the drive-by other entities to contribute to the sustenance of cloud computing the major challenge that needs much concern is data security [6]. This is attributed to the varying architecture and designs used in cloud computing such as software, hardware, and Application Programming Interfaces [7]. The differences in configuration make cloud clients and providers face diverse issues relating to security [6], and [7]. Jibir et al. indicated that variants of attacks as well as threats

Journal of Theoretical and Applied Information Technology
31st March 2023. Vol.101. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are targeting the cloud now and then [8]. Imperva which is a well-known company that provided cyber and data security warned its customers of an impending attack on cloud applications called man-in-the-cloud [8].

1.1 Services and Cloud Deployment Models

The various service models of cloud computing and a brief review of cryptographic schemes are discussed in this section.

1.1.1 Software-as-a-Service (SaaS)

The delivery of software on a subscription base by a third party to multi-tenants is considered Software-as-a-service. These systems deploy software once and can be accessed by clients both from smaller to large entities. There is always an integrated system used over the internet which might require routine modification and novel activities [11].

1.1.2 Platform-as-a-Service (PaaS)

Platform-as-a-Service makes available an environment that allows applications, the development of the applications, and maintenance of the applications [12]. The cloud clients can create, plan, improve and assess the developed applications directly from the cloud and monitor the applications' development cycle.

1.1.3 Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a -service serves as the basis upon which all other cloud services are built. This replaces the traditional data centers in the normal network architecture. Cloud service providers use this model to provide platforms upon which cloud client can store their resources [13]. Cloud clients resort to IaaS on the basis that the cloud service provider can sustain the quality of the service they provide. The guarantee for the usage of IaaS is explained through the Service Level Agreement (SLA) which is linked to the lifecycle of the cloud service provider and shows the monetary as well as procedural dynamism relating to SLA as shown in Figure 1.

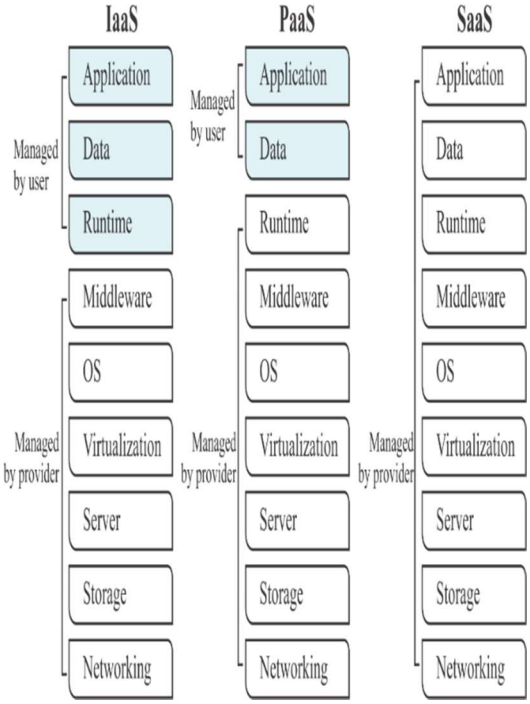

Figure 1. Management of resources in cloud computing [14]

1.1.4 A Container-as-a-Service (CaaS)

Container-as-a-Service allows developers to use a package for their entire programming task. The container contains all the coding needs, run timing, and configuring together with the libraries the system needs to execute a host machine [15].

A container-as-a-Service provides all the libraries that are needed to run a program and are not dependent on any other virtual system for the needed libraries as indicated in Figure 2. They can provide a whole unit for uploading, organizing, running, scaling, and managing the container.

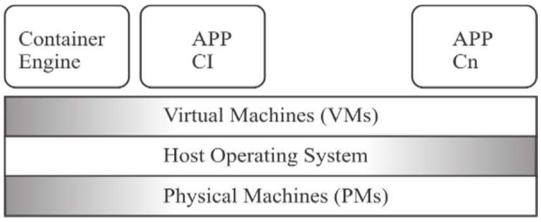

Figure 2: Container as a Service architecture [15]

1.2 Cloud Deployment Models

The uniqueness in accessing resources that are shared on the cloud is considered cloud deployment models. Based on this four different models are considered namely;

1.2.1 Public cloud

This is a type of cloud that allows entities to access data using the internet depending on their common goal and allows applications to be made available to the group with the help of servers in the cloud [16]. Such clouds are provided for the general public and they are under the control of governmental organizations, businesses, academicians, or the blend of all units hosted by a cloud service provider on its site [17].

1.2.2 Private cloud

According to [18], private clouds are meant for the storage of personnel or the execution of a task by a distinct entity. Such a cloud particularly stores very sensitive means or monetary data of the entity thereby making it a patented platform. Private clouds are used as single entity schemes and their operations are based on already existing infrastructure or new resources which are located on the organization's premises under the care of a third–party company [19].

1.2.3 Hybrid cloud

The blend of the economies and competencies of public and private clouds results in a hybrid cloud that provides the advantages of data security for the two infrastructures [20]. According to [21], their merger requires more technical skills in terms of their collection, analysis, assessment, and the entire managerial task of hybrid platforms. There are a lot of challenges associated with hybrid clouds which include data security and governance.

1.2.4 Community cloud

The community cloud is considered a multi-tenancy platform aimed at allowing companies to leverage a common resource [22]. Such a type of cloud allows the users to work on a common project because they have one goal to attain using the software of the community as indicated in Figure 3. On this platform, tenants are all concerned with common security as well as the principles of agreement among them with a delegation of monitoring and assessment by a third party [23].

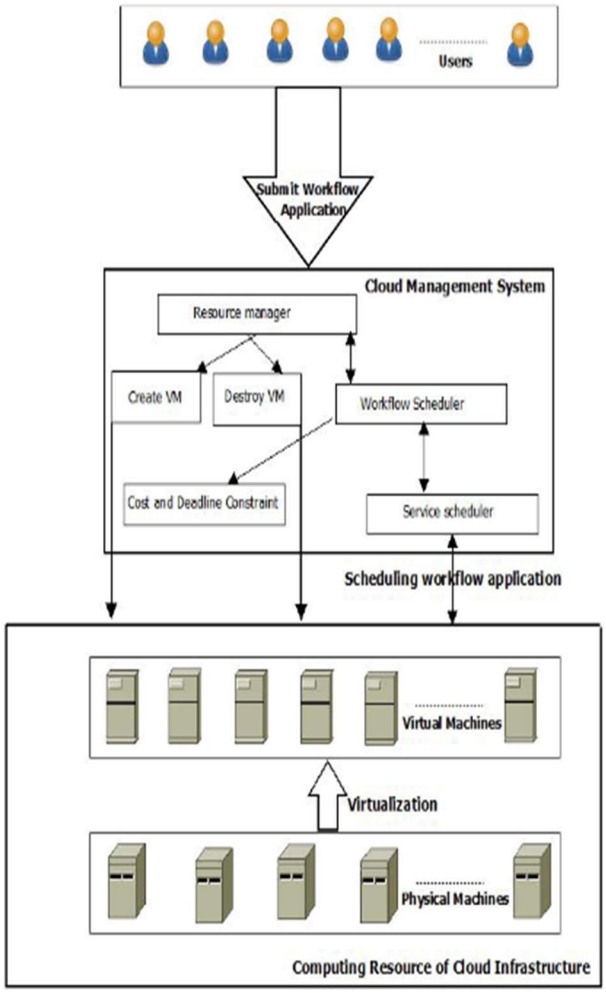

Figure 3. Scheduled Workflow On A Community Cloud [24]

1.3 Cloud Client

Cloud clients are individuals or companies that utilize the resources of a cloud service provider. They have the utmost right to choose the services of any service provider and pay them according to services rendered to them (cloud client) by the service provider after which their contract ends. A service level agreement is made by the cloud client in determining the quality of the service rendered [40]. These agreements are signed relating to the quality of service, confidentiality, prevention, and integrity of the service provider.

1.4 Cloud Service Providers

Cloud Service Providers (CSP) are entities that render computing as a service to cloud clients. The management of all the cloud services and the infrastructure is under the control of cloud service providers [41]. Software-as-a-Service and

Infrastructure-as-a-Service cloud providers are responsible for the provision of resources to cloud clients through organizing, arranging, sustaining, and keeping up-to-date applications as well as the management of infrastructure. The cloud service provider provides all the architectural design and the computing infrastructure such as networks, servers, and the hosting of all the infrastructure as shown in Table 1 [42].

Table 1. Various Performers In Cloud Computing [39]

Performer	Function
Cloud Client	An entity that uses the services rendered by a cloud service provider based on a subscription base.
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 subscribers and cloud service providers seeing to the worth of their services delivered.
Carrier of Cloud	Any organization that ensures connectivity between cloud clients and cloud providers for the transport of services offered.

1.5 Security Challenges in Cloud Services

1.5.1 Security in Software-as-a-Service

This is the interactive layer in cloud computing which makes all security challenges to be linked to data in cloud computing [25]. Security-as-a-Service stresses the duty of the cloud client to provide the needed security for the data off-loaded by putting in checks on who can access such data and also the security schemes that could be employed by the cloud service provider. The commonest security issues associated with Software-as-a-Service are; the problem with configuration, the problem with complying with regulations, and the problem of recovering from disaster.

As a result of the above issues, researchers need to consider the relationship in terms of security between cloud providers and providers of SaaS. There are, therefore, calls for proper scrutiny of the security approaches used by cloud service providers.

1.5.2 Security in Platform-as-a-Service (PaaS)

According to [26], there are three divisions for Platform-as-a-Service which are the layer that links with Software-as-a-Service which is the intermediate layer purported for storing an application, data run timing management for database, and the last layer for backend activities such as network, storage, and CPU storage. The security issues as suggested by [27] against Platform-as-a-Service are; hacking and attacks, poor data visibility, abuse of cloud services, and encryption and authentication bypass. From these security issues, cloud service providers should ensure that proper identification and verification mechanisms are put in place to ensure a greater security door in PaaS.

1.5.3 Security in Infrastructure-as-a-Service (IaaS)

This is the service level that allows cloud clients to make use of virtual devices for storing data and optimizing the use of the Central Processing Unit (CPU). The layer faces a lot of security challenges based on the frequency of accessing the service. Some of the security challenges put forward by [28] are; leakages of data, loss of data, insider attacks, and inadequate visibility.

The need for proper legal terms and regulations for the activities of cloud clients in the usage of IaaS is suggested.

1.5.4 Security in Container-as-a-Service (CaaS)

The use of the Container-as-a-Service has increased because of the numerous advantages derived from it such as being light, faster, simple deployment, better utilization of resources, and the control of version [29]. Some of the security challenges in CaaS are container malware and container privilege insecurity. To make Container-as-a-Service more secure the Operating System kernels must be more robust in terms of security since clients are allowed to share the same Operating System [29]. The various cloud security challenges and issues are outlined in Table 2.

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 data control
Platform-as-a-Service (PaaS)	i. Accessing a 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 iv.	i. Security issues relating to Service Level Agreement ii. Security of providing software using network
Container-as-a-Service (CaaS)	i. The sharing of operating systems used by the host possess a security threat ii. Security of apps in the container	i. Critical concentration on runtime is needed ii. Securing container-to-container activities

1.6 CLOUD SECURITY ISSUES

1.6.1 Confidentiality

Securing data from unapproved persons to have access to the data is considered confidentiality [30]. Many researchers have used varying techniques to achieve this, ranging from cryptography to the combination of cryptography to dividing into blocks [31]. Examples of security schemes used to ensure the confidentiality of data are;

1.6.1.2 Encryption using a biometric approach

In this approach varying parameters such as voice signals, iris of the eye, face recognition, and fingerprint scans are used. These schemes are very distinct and difficult to manipulate so they prevent access to the stored data [33].

1.6.1.3 Using the classification approach of K-NN

The use of the supervised machine learning algorithm K-NN is also considered an alternative to achieving the confidentiality of data as proposed by [34]. This is mostly used in the recognition of patterns, segmentation of data, forecasting as well as an approximation which aims at selecting profound data that helps in attaining data confidentiality.

1.6.1.4 A secure scheme using HPI

Cloud clients are allowed to save data on the cloud by applying the security scheme of Hypertext Transfer Protocol (HTTP) in this approach [31]. Data obtained is scrambled after which it is moved to the cloud and unscrambled upon request by the cloud subscriber from the cloud. This raises the confidentiality of cloud data using the end-to-end encryption scheme.

1.7 Integrity

Data integrity ensures the reliability of customers' data which indicates that their data are safe and have not been altered as appropriate cryptographic algorithms have been adopted [32]. The concern of data integrity is to prevent the loss of customers' data. This is very important due to frequent access to data by customers from the cloud service provider. Examples of appropriate security approaches to attain data integrity on the cloud includes planning for business continuity, and regular backups.

1.7.1 Verification based on BLS signature

Boneh–Lynn–Shacham (BLS) signature is a security scheme used to ascertain the authenticity of a signer. A bilinear pair is what this scheme uses for authentication and is based on the basics of an elliptic curve. This makes it more secure against the attack of the index and was employed in the works of [54]. Their scheme had five stages of verifiability which are, Key Generation, Token Generation, Challenge, Response, and Check Proof. These approaches support auditing verification as such ensure proper verification.

1.7.2 Blockchain

Blockchain has been considered an alternative to cryptosystems for ensuring data integrity on the cloud. This is evident in the study of [55] where an integrated mechanism of

Blockchain-based linear mapping was used. This helped to overcome the trust concerns of Third-Party Auditors reducing huge computational and connectivity overheads. The message is sliced and homomorphic verifiable, and tags are produced for the sample verification.

1.8 Availability

Data availability ensures the readiness of data stored on the cloud to its owners. This aims at a holistic retrieval of data. The cloud client wants to be sure that the cloud service provider has not succumbed to the data at their end, which might have resulted from device failures, software bugs, and other threats of the cloud that could have any effect on the data [56]. In recent times, data availability is achieved by replicating data on two or more virtual servers upon configuration by the cloud client. Some leading organizations that offer multi-data duplication at different geographical locations are Amason S3 and Google Cloud [57].

1.9 Techniques Of Data Security In The Cloud

1.9.1 Firewall

To ensure the prevention of host and network attacks on the cloud, firewalls are installed which makes it an effective security approach that can be used to ensure security in the cloud. A firewall can assess as well as regulate the connectivity of devices [50] which helps to prevent attacks such as Economic Denial of Sustainability (EDoS) and cross Virtual Machine (VM) [51]. This helps to protect the entry of Autonomous architecture into the cloud network by protecting inside nodes from external attacks which helps to ensure the security of the system. As a result of the dynamic nature of cloud computing, the firewall can shade the inside and outside security properties which could be achieved by allowing outside entities that utilize rented instances by executing the rented firewall software [51]. This is making the use of a firewall very secure to ensure cloud data security and privacy.

1.9.2 Encryption

In securing data on the cloud, appropriate cryptographic algorithms are used. Cryptographic algorithms scramble the plaintext to an unreadable form [52]. The strength of such algorithms depends on the encryption key that is used to execute the encryption process. An algorithm like the RSA which was proposed by Rivest, Shamir, and Adleman in 1978 has its strength based on prime number factorization which is difficult to compute by the attacker using discrete logarithm time. There are a series of cryptographic algorithms that are used to secure the cloud such as Advanced Encryption Scheme (AES), Data Encryption Standards (DES), and Blowfish. Other integration approaches include Blowfish and AES, SHA1, and DES. All these are employed to ensure the security of the cloud. A brute force attack is considered the commonest attack on cryptography.

1.9.3 Data Masking

The process of hiding real data from its natural structure making it un-genuine to prevent leakage of data is termed Data Masking. It is seen as an intermediary between encryption and the token approach. Data masking has the property of hiding the original data by obscuring some elements in the message that unintended users are not expected to see [53]. This approach allows for offshoring, allocating, and affiliating as well as using cloud solutions based on legal boundaries. Two types of data masking are considered namely dynamic and static masking. Dynamic masking is the application of a selective hiding technique based on legal rules considering the viewers of the data giving security to delicate data similar to the plaintext with no scrambling property. Static data masking ensures holistically hiding the content from unauthorized persons making the data not revocable.

1.9.4 Blockchain(Distributed Ledger Technology)

The ever-growing technology which authors have suggested to have the capability to potentially secure data in this information-growing era is Blockchain. In Blockchain a list of blocks is arranged in hierarchical levels making it cryptographically secured. Blockchain activities are arranged in a peer mode using the connectivity of computers distributed globally [58]. Each computer in the network keeps a copy of the mirrored data which guards against data loss, editing, or data tampering which helps to raise the security of data managed using Blockchain.

In an attempt by researchers to handle these security issues properly, several research studies have been done as in Dinh and Park, and Saravanan and Umamakeswari, [9] and [10]. Though there are situations where modern cryptographic algorithms could be used to

increase security in the cloud, current approaches are not able to withstand current security threats that attack the client and the provider end in recent times because of the high execution time of the algorithms.

From what has been said so far, it is evident that some pertinent issues hinder the security of data on the cloud. This study, therefore, aims at surveying various works of previous research in areas such as the most used approach to secure data on the cloud, the types of cryptographic algorithms employed, the purpose of these cryptographic algorithms to achieve security in the cloud, and the security concerns in the cloud.

2. RELATED WORKS

Security in the cloud has gained much attention from researchers. Series of conferences have been organized by The 2nd International Conference on Electrical, Communication, and Computer Engineering; 2nd World Congress on Computing and Communication Technologies; and ACM International Conference Proceeding Series, (2020) among others are some of the various conferences that concentrated mainly on cloud computing security. Not only that but also many journals have published works by eminent researchers on cloud computing. In this section of the current study, a detailed review of articles that concentrated on surveys of cloud security issues is discussed.

According to [35 their research investigated the security mitigation and threat approaches used in cloud computing, and they identified that the most highly researched area of data security is leakage and tampering of data. In addition, they indicated that intrusion detection was among the security challenges of cloud computing.

Again [35] disclosed that another major challenge facing cloud clients and cloud service providers is waving their sensitive data to a third party to store. One thing worth mentioning about the findings from [35] is that even though they used a different approach in their study, they embraced the Blockchain scheme to ensure data security. However, in their support for the Blockchain scheme, they have advocated for more research into an appropriate approach to ensuring better confidentiality, integrity, and availability of data.

In the study by [36], detailed survey work on cloud security challenges was conducted. In that study, several security challenges such as cloud architecture, cloud concept, and the provision of structures that can be employed to achieve data privacy were investigated. Further analysis of various security schemes such as ABE, KP-ABE, searchable encryption, and other approaches was also considered. In summarizing [36], proposed that, for data privacy, legal entities like HIPAA (Health Insurance Portability and Accountability) and FAPA (Financial Agency Privacy Act) should provide stringent legal frames to ensure data privacy as done in many countries.

The study of [37], did an intensive review of papers based on keywords like security and privacy of e-health data on the cloud, HER architecture as well as cryptographic and non-cryptographic schemes used in HER. In their study, they placed much attention on the challenging issues and advantages of the cloud though they advocated for further research in the area of cloud data security and privacy of e-health. They also indicated that an intensive study of the security of e-health using the cloud could attain the integrity and confidentiality of the data on patients.

Yang et.al [38] indicated that there had been intensive studies on security challenges and privacy in cloud computing but there is still a gap in the literature. An all-inclusive survey was conducted digging into eight data security elements namely; confidentiality, integrity, availability, fine-grained access control, safe data sharing in groups, and data leakage - resilience. Two major challenges were identified by the paper. The dishonesty of parties makes them not to be able to share data and cloud clients with fewer facilities might not be able to undertake operative data mining activities. Aside from these, suggestions in the summary indicated the proposal of a robust data privacy scheme and a safer scheme for outsourced data using an appropriate machine learning scheme.

The study by Basu et al. [39), revealed that a major challenge in cloud computing is the security of the cloud which much research has been conducted on but there is no clear linkage between the cloud data security at hand and the suggested solutions such as Blockchain and cryptographic schemes. There is a lack of unit schemes for achieving the problem of virtualization and the control approaches identified by [40] on cloud security and the proposed solutions provided a common platform to meet an exact need to solve the problem of

cloud security [41]. To add on, the solutions stated in the survey of [42] did not state the exact challenge it handled. [39], proposed that a better robust approach should be developed that can handle specific security challenges in cloud computing.

Rajeswari and Kalaiselvi [43] researched data storage in the cloud by assessing data security relating to integrity, access control, and the use of attribute-based encryption. From their work, one major conclusion was that the computation overhead for data storage and security should be less though the security of the cloud could be attained better through verification, approval, privacy, and integrity.

Pavithra et al [44] also surveyed cloud security challenges using Blockchain. Their work suggested that the use of Blockchain has the security strength to curb cloud security concerns. Their work, therefore, assessed and related security challenges by utilizing Blockchain. They concluded that increasing device connectivity, as well as calculations, will serve as the solution to security challenges in the cloud.

Sevis and Seker (45) surveyed ensuring the integrity and security of data in the cloud. In their work, they drew much attention to untrusted servers and unapproved individuals who can or might take advantage of the data left in their care. Their concern was that as data is kept in a remote infrastructure under the control of a third party, that data can be altered, detached, dishonored as well as pilfering. They concluded that for cloud computing to be secure, its design must be well-organized, be multi-tenant computation, be dynamic, able to retrieve data stored, and have an enhanced security scheme.

Saxena and Chourey [46] concentrated on security in the cloud and the corresponding challenges that arose. They identified that, as the cloud is hosted over the internet it makes it prone to a lot of vulnerabilities relating to its execution and security challenges. Their paper suggested that, though cloud computing is a complex system, data privacy can be attained when model-by-model level concentration is used.

Nagesh et al. [47] also indicated that data integrity, privacy, and security can be considered as some of the challenges hindering the full adoption of cloud computing by companies and other entities. Their work cited solitaire cloud to be more vulnerable compared with multi-tenant cloud systems on which much research has not been done. After they had compared their work with other research works, they concluded that the multi-tenant cloud is at the developing stage and a stronger architectural design could help bring solutions to the problems of data security as well as client privacy. Such a decision by [47] could provide efficiency in calculations, connectivity, and dynamism in operation.

Patel [48], considered data confidentiality as the major security challenge in cloud computing. Patel analyzed various algorithms that could be used to achieve confidentiality of data such as encryption using biometrics, Secret Sharing Schema, and K-NN classification. It was suggested by [48] that the use of encryption and obfuscation techniques is the best approach to ensure the confidentiality of data in the cloud.

Mahboob et al [49], in their study, stated that among other things, the most highlighted security challenge in cloud computing is client authentication and access control. They suggested that to control this challenge they should use a robust scrambling technique. In their future works, they thought of placing much emphasis on utilizing a high-scaled scrambling scheme that could help them to achieve a more secure cloud.

Kaura and Lai [50] suggested that with the increase in the number of devices connected to the cloud, security is the highest challenge. Their study discussed the various services in the cloud, their associated risk, and the mitigating factors utilized to ameliorate them.

From the review of available literature by various authors, the security of the cloud which is the major concern points to data integrity, confidentiality, availability, and access control. Researchers have proposed varying approaches ranging from Blockchain to encryption schemes aimed at ensuring the security of the cloud. Dishonesty of third-party entities and cloud clients has also been identified as leading to cloud insecurity. Legal entities like FAPA and HIPAA should propose stringent measures to ensure data privacy. Finally, the current study observed that no African writer has published a document concerning cloud computing challenges and this is a gap to be filled. The current study aims at filling that gap.

3. METHODOLOGY

In this survey, the Systematic Literature Review which is based on Prisma is used to assess the number of research directed toward cloud data security. Graphs and tables are used to interpret the data obtained.

3.1 Research Questions

The objective of this study rests on evaluating issues of security in cloud computing through security interventions proposed by researchers were also considered. Six goals were considered for this research. These objectives were;

3.1.1 Which cryptographic scheme was mostly employed by researchers to secure data on the cloud?
3.1.2 Which cryptographic algorithms were used to secure data on the cloud?
3.1.3 How did cryptographic schemes encrypt and decrypt data on the cloud?
3.1.4 What was the execution time trend of the cryptographic algorithms (linear time / non-linear time) used?
3.1.5 What were the intended aims of these cryptographic schemes?
3.1.6 What were some of the security concerns in cloud computing?

3.2 Approaches for Accessing Articles

In this section, the researcher placed much attention to various phrases, databases, and referencing tools used. The processes for the search which has been discussed in detail as follows;

3.3 Phrases Used

A Series of phrases were used in arriving at the various articles used in this survey. The topic-related phrases used to retrieve the various articles from various databases included; “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

Some well-known digital sources which were used in scouting for articles for this survey include Taylor and Francis, Scopus, Research Gate, Web of Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, and ACM.

3.3.2 Reference Management

A large volume of articles was downloaded based on the keywords used for the study. The IEEE reference generation tool was used as the management tool for the referencing of these articles which helped the researcher in the collation of the articles.

3.3.3 Search Processes

The researcher searched popular digital libraries to download articles that are related to the topic under consideration. The articles were publications from conferences as well as books. All 157 papers were downloaded by the researcher and were organized using the IEEE reference generator. This allowed for easy tracking of the downloaded papers which eased the referencing and then presented in a Prisma framework [59]. A selection procedure was used to group the downloaded papers based on their relevance to the study. Out of the 157 papers downloaded, 72 were considered relevant to the topic under review. The exclusion procedure used for the selection of the papers of interest was;

I. Papers with publication dates earlier than 2015
II. Papers with no DOI
III. Papers that concentrated on cloud taxonomy
IV. Articles that used anonymous citation
V. Papers that concentrated on Blockchain technology rather than those that concentrated on cloud computing security

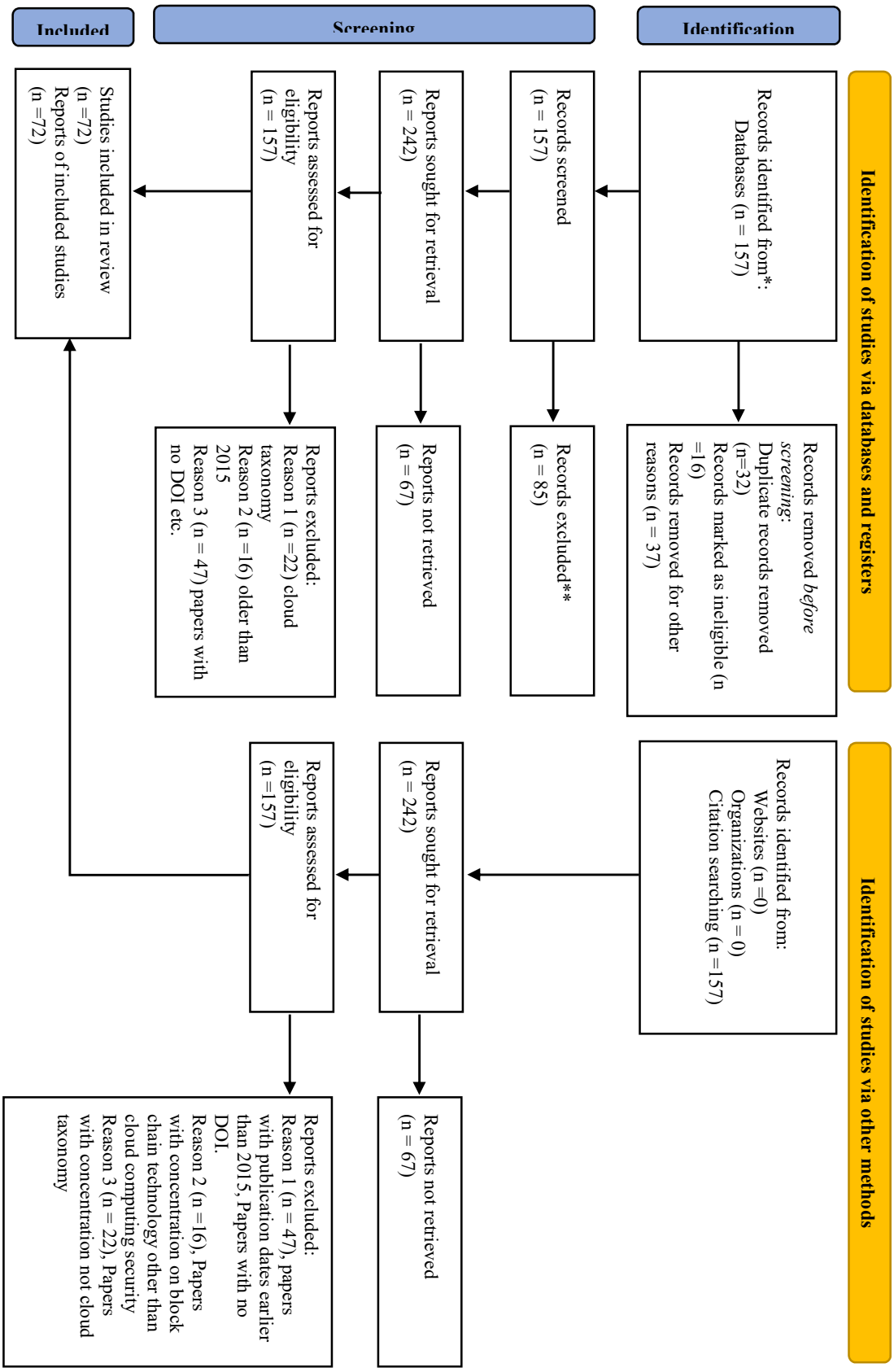

Figure 4. Flow Diagram For The Systematic Review Which Included Searches Of Databases, And Other Sources [59]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4 RESULTS AND DISCUSSION

This segment presents the Systematic Literature Review outcomes and their discussion.

4.1 Which Cryptographic Scheme Was Mostly Employed By Researchers To Secure Data on The Cloud?

In Figure 5, the most used approach to ensure cloud security is encryption schemes which make up 16.7% of the publications used in this survey between 2017 and 2021. These encryption schemes used existing cryptographic algorithms and hybrid algorithms. This was followed by the use of encryption models indicating a percentage of 9.7% of the survey papers. The most utilized encryption model adopted by researchers to secure the cloud was based on the Map-reduce layer using a Hadoop platform [61].

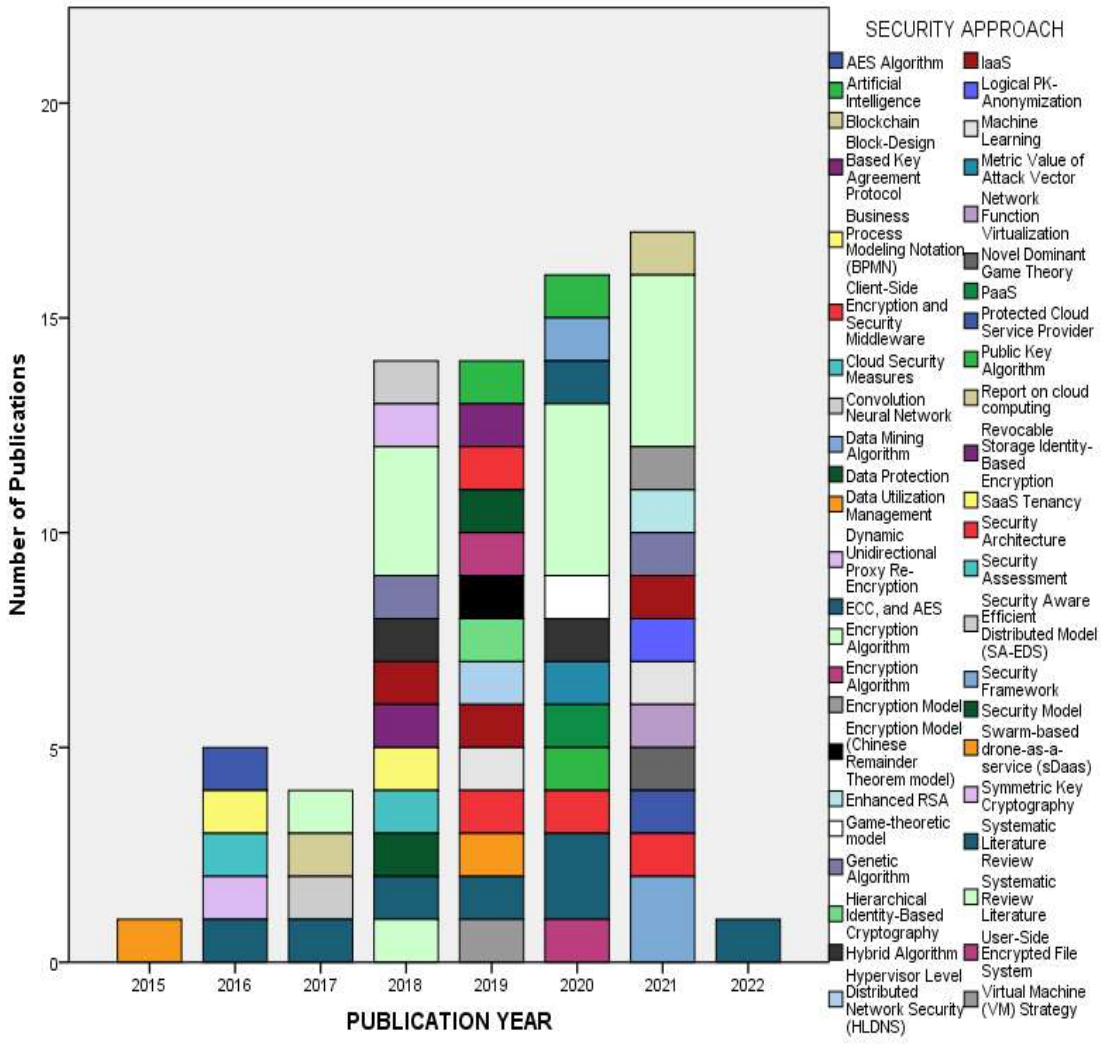

Figure 5. The Most Employed Cryptographic Scheme Used To Secure Data On The Cloud

4.2 Which Cryptographic Algorithms Were Used To Secure Data on The Cloud?

Figure 6 depicts the various types of cryptographic schemes used to secure data on the cloud. These are categorized into asymmetric and symmetric algorithms. From Figure 2.6, in 2016, 2% of each of the published works used in this survey were based on both symmetric and asymmetric properties. This was increased to 5% for asymmetric algorithms and 4% for symmetric algorithms. There was a significant increase in proposing the use of an asymmetric algorithm to secure data on the cloud in 2021 with a percentage of 8% and 7% for symmetric algorithms. There was a drastic decline in 2022 from 8% in 2021 to 0% in 2022 for asymmetric algorithms and from

7% in 2021 to 1% in 2022 for symmetric algorithms.

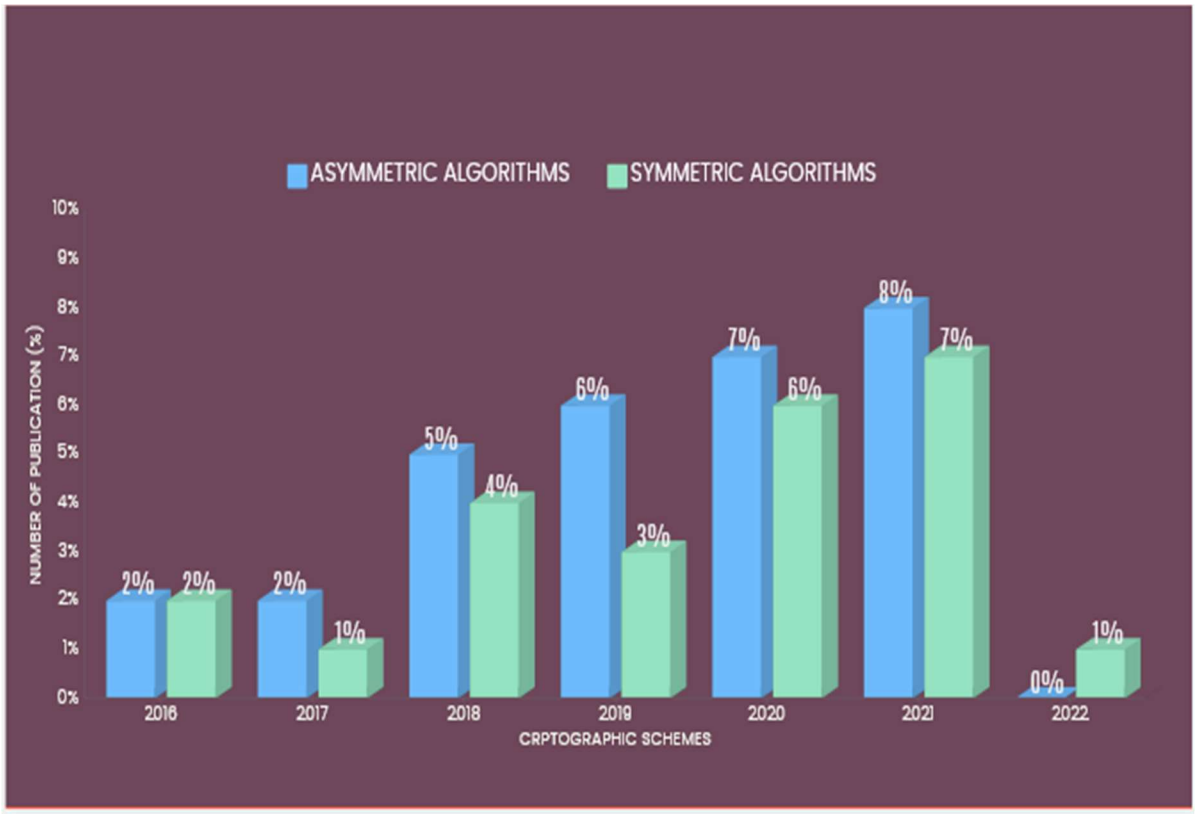

Figure 6. *Type Of Cryptographic Algorithms Used To Secure Data On The Cloud*

4.3 How Do Cryptographic Schemes Encrypt And Decrypt Data on The Cloud?

The encryption and decryption of data on the cloud are achieved in two ways. The first approach is encrypting the whole data as a block which is termed block ciphering or executing the data alphabet by alphabet which is also termed stream ciphering. From Figure 7, 4 % of algorithms proposed in 2016 employed a block cipher approach while 0 % of the survey papers used the stream cipher technique. However, the usage of block cipher algorithms escalated to 10 % in 2020 with a corresponding 2 % increase for stream cipher algorithms. In 2021 there was a decline in the usage of block cipher algorithms from 10 % in 2020 to 9 % in 2021 with an increase in the usage of stream cipher algorithms in 2021 with a percentage of 7 %.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

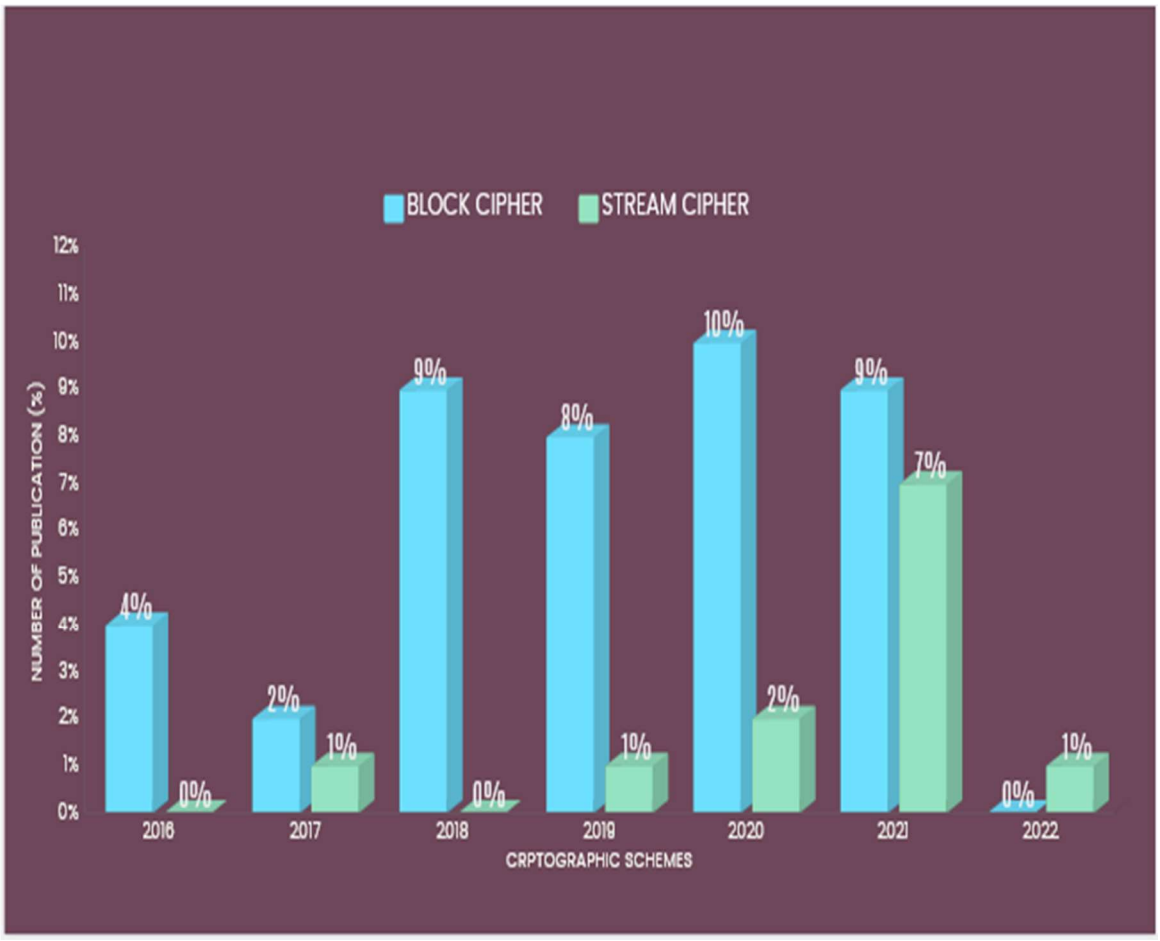

Figure 7. How Cryptographic Schemes Encrypt And Decrypt Data On The Cloud

4.4 What Is the Execution Time Trend of the Cryptographic Algorithms (Linear Time / Non-Linear Time) Used?

The execution time trend measures the performance of an algorithm on the time it takes to scramble and decrypt data using different data sizes [61]. The performance evaluation of an algorithm is categorized into linear and non-linear execution time. The Linear performance evaluation is observed when the execution time of the algorithm is proportional to the data size. Thus the higher the data sizes the higher the execution time as indicated in the study of Pereira et al., [62]. However, the non-linear algorithm performance is not based on data size but on the size of the nonce value used during the execution of the algorithm [63]. From Figure 8, in 2016 there was a 1 % usage of linear as well as 1 % usage for non-linear algorithms. There was an increase in the usage of linear algorithms in 2020 from 9% to 12%. There was no increase in the usage of non-linear algorithms which was still at 0%. Researchers 2021 did a lot of work on linear algorithms resulting in a 14% increase but there were no proposed non-linear execution time algorithms in 2021.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

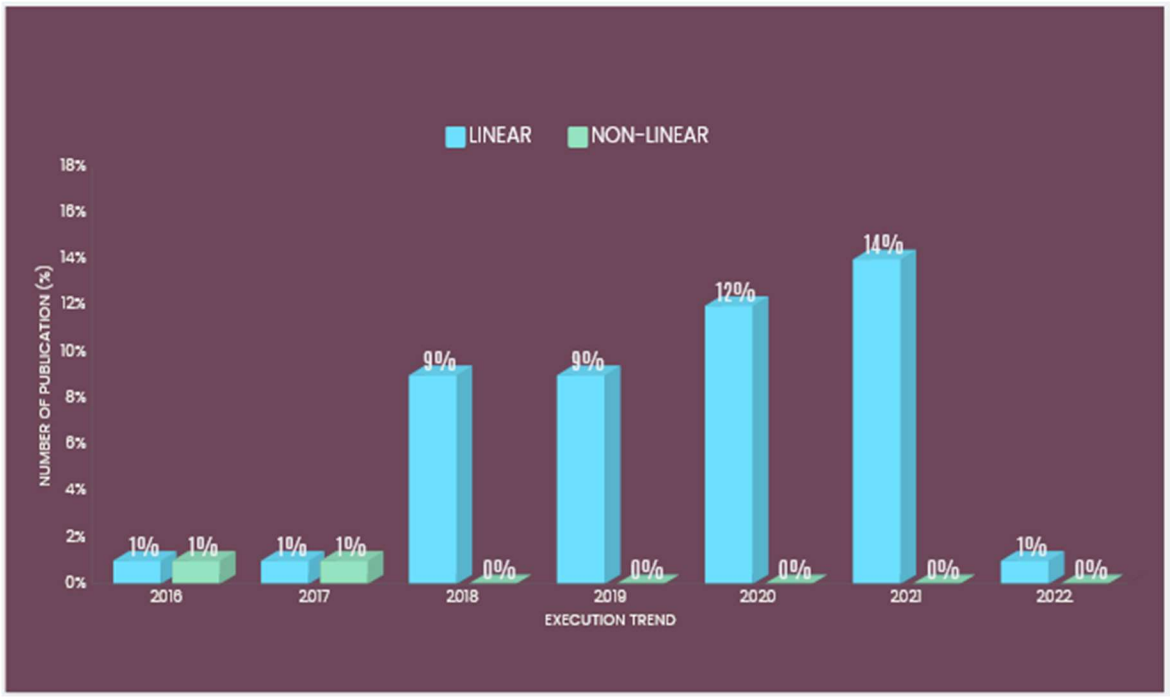

Figure 8. Execution Time Trend Of Cryptographic Algorithms Used To Secure Data On The Cloud

4.5 What are the intended aims of these cryptographic schemes?

Figure 9 shows the main objectives for the employment of the various cryptographic approaches. Cryptographic approaches are mechanisms used to control the security challenges in the cloud such as privacy preservation, cloud security, the confidentiality of data, and others. From Figure 9, ensuring data security on the cloud had 30.6% of all the publications involved in this survey from 2015 to 2022. Figure 9 and Table 3, depict that ensuring data security on the cloud has 30.6% of all the publications involved in this survey from 2015 to 2022. This is supported by the study that [35], [37], [38], [43], [44], [45], and [47] data security has been the biggest security concern of researchers. This was followed by cloud security which had 29.2% of the total publications used in this Systematic Literature Review.

The study by Kaura and Lal [50] supported this viewpoint. From Figure 9, only 2% of the papers reviewed concentrated on ensuring data confidentiality which is supported in the study by Patel [48]. The least of the mechanism used is aimed at penetration testing and anomaly detection on the cloud and had 1% in 2019.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

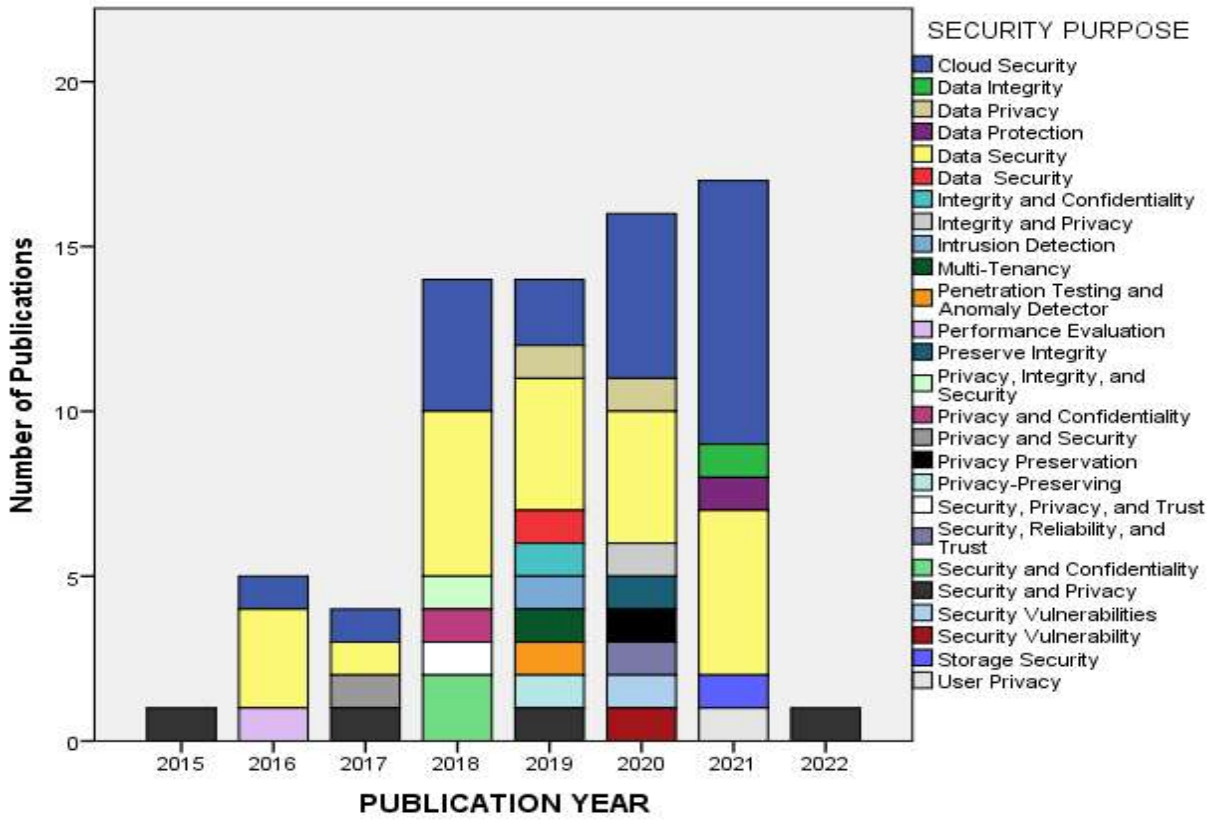

Figure 9. Intended Aims Of Cryptographic Schemes

4.6 What Are Some of The Security Concerns In Cloud Computing?

Cloud users and cloud services providers raised a lot of factors related to data confidentiality, data privacy, data integrity, and many more aside from the benefits associated with cloud computing. These security concerns have made clients not fully migrate onto the cloud [130]. Gartner categorized cloud security risk into seven (7) groups [133].

The categorizations according to Gartner's security risks are;

I. Access Control: Access control manages the in and outflow of access to data by cloud clients'.
II. Governance: Clients' data security and integrity are controlled by governance.
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 available anytime it is needed by the cloud client.

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

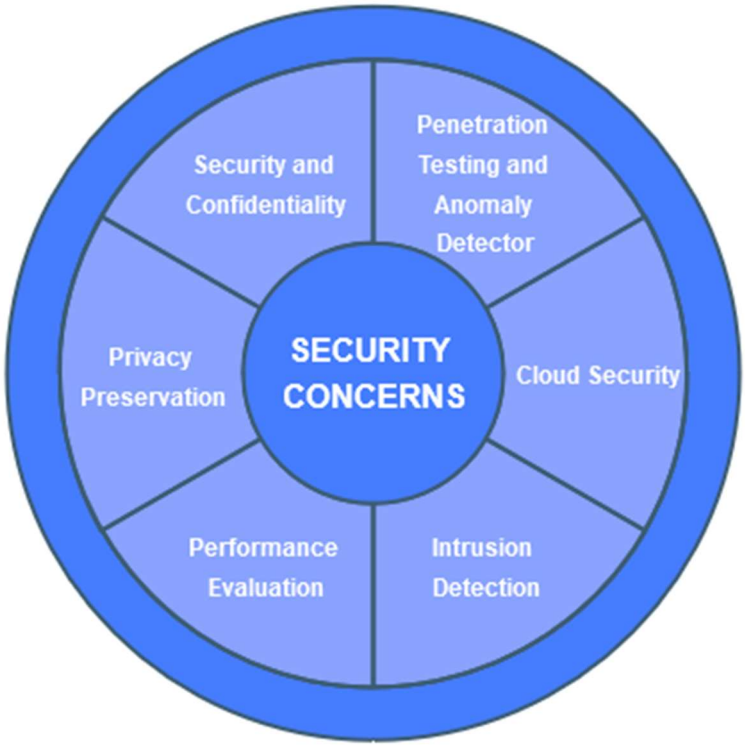

Figure 10. Security Concerns In The Cloud

Table 3, depict the various publications which were surveyed from renowned databases such as Taylor and Francis, Scopus, Research Gate, Web of Science, IEEE Xplore, Science Direct, Hindawi, Google Scholar, and ACM.

Table 3. Papers Used In Survey

ARTICLE REFERENCE	CRYPTOGRAPHIC SCHEME	PURPOSE
[64]	Encryption Algorithm	Data Security
[65]	(Protocol) Game-theoretic model	Attack on the cloud
[66]	Chinese Remainder Theorem	Privacy preservation
[67]	Model Driven Engineering techniques	Security analysis
[68]	Encryption Algorithm	Data security
[69]	Encryption Algorithm (AES and RSA)	Data protection
[70]	Encryption Algorithm	Data Security
[71]	Protocol (Security Framework)	Data Security
[72]	Machine Learning Algorithm	Cloud Security
[73]	Business Process Modeling Notations	Cloud Security
[74]	Security Framework	Cloud Security
[75]	Security Framework	Intrusion Detection
[76]	Security Mechanism	Cloud Security
[77]	Security Framework	Cloud Security
[78]	Security Framework	Data Security
[79]	Security Strategy	Cloud Security
[80]	Virtual Memory Deployment Approach	Data Security
[81]	Encryption Algorithm	Data Security
[82]	Encryption Algorithm	Data Security

[83]	Machine Learning Algorithm	Data Security
[84]	Encryption Algorithm	Data Security
[85]	Security Framework	Security, Privacy, and Trust
[86]	Encryption Algorithm	Data Security
[87]	Security Framework	Cloud Security
[88]	Encryption Algorithm	Data Security
[89]	Encryption Algorithm	Data Security
[90]	Encryption Scheme	Data Security
[91]	Security Framework	Cloud Security
[92]	Security Framework	Security and Privacy
[93]	Encryption Technique	Cloud Security
[94]	Encryption Algorithm	Cloud Security
[95]	Security Framework(Map Reduce methods)	Cloud Security
[96]	Encryption Algorithm	Cloud Security
[97]	Encryption Scheme	Cloud Security
[98]	Encryption Scheme(Chaotic Searchable Encryption)	Cloud Security
[99]	Security Framework	Privacy and Security
[100]	Security Framework	Cloud Security
[101]	Blockchain	Cloud Security
[102]	Encryption Algorithm	Cloud Security
[103]	Security Framework	Cloud Security
[104]	Encryption Algorithm	Cloud Security
[105]	Encryption Algorithm (AES and key agreement protocol	Cloud Security
[106]	Encryption Algorithm	Data Privacy
[107]	Blockchain	Security and Privacy
[108]	Encryption Algorithm	Cloud Security
[109]	Security Framework	Security and Confidentiality
[110]	Encryption Algorithm	Cloud Security
[111]	Encryption Algorithm (AES)	Cloud Security
[112]	Encryption Algorithm (AES)	Data Security
[113]	Encryption Algorithm (AES)	Cloud Security
[114]	Encryption Algorithm	Cloud Security
[115]	Encryption Algorithm (RSA)	Cloud Security
[116]	Encryption Algorithm (RSA)	Data Security
[117]	Security Framework	Cloud Security
[118]	Encryption Algorithm	Data Security
[119]	Encryption Algorithm	Data Security
[120]	Security Framework	Data Security
[121]	Security Framework	Data Security
[122]	Security Framework	Cloud Security
[123]	Encryption Algorithm	Data Security
[124]	Encryption Algorithm and Data Mining approach	Cloud Security
[125]	Encryption Algorithm	Cloud Security
[126]	Security Framework (Security-Aware Efficient Distributed Storage (SAEDS) model)	Cloud Security and Privacy
[127]	Encryption Algorithm	Security and Confidentiality of Cloud Data
[128]	Security Framework	Cloud Security
[129]	Encryption Algorithm	Cloud Security
[130]	Security Framework	Data Security
[131]	Security Framework	Security and Privacy
[132]	Security Framework	Security and Trust
[133]	Security Framework	Cloud Security
[134]	Encryption Algorithm	Data Security
[135]	Security Framework	Cloud Security
[136]	Security Framework	Cloud Security

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5 CONCLUSION

In this survey, a Systematic Literature Review was conducted to review the existing literature relating to cloud computing however, much emphasis was placed on the security approach which is mostly employed to control security challenges in the cloud. The type of encryption algorithms used to secure the cloud, how algorithms encrypt and decrypt data on the cloud, the execution time trend of the algorithms used in the cloud (Linear time / Non-Linear time), the intended aims of security approaches, and some of the cloud concerns in cloud computing were also not out in the study. A lot of security techniques used to secure data on the cloud were identified which include firewalls, data masking, encryption, and Blockchain. The survey also identified some security challenges in cloud computing and identified approaches that are used in accomplishing such security challenges. The security challenges identified were confidentiality and privacy which could be addressed through encryption using the biometric system, the classification approach of K-NN, and a secure scheme using HPI. Data integrity as a security challenge could be controlled through verification based on BLS signature, and Blockchain. The availability of data was also identified as a security challenge in cloud computing and this can be attained through data replication on different servers. The migration to the cloud comes with its advantages for cloud clients, and cloud service providers but maximizing these profits calls for proper and sustaining security approaches to tie the breach of security concerns in cloud computing. This systematic literature review shows that security is a major setback to the full adoption of cloud computing both on the part of the cloud client and the cloud service provider.

Moreover, the survey identified that the best approach to ensure cloud security is through the employment of encryption algorithms. According to the survey, of all the publications considered, the encryption algorithms proposed from 2016 to 2022, 90% of them had linear time complexity. This makes their execution time to be predictable and dependent on the size of the data.

For future research, this study suggests that much attention should be diverted to researching data security, data privacy and confidentiality, reliability and trust, and multi-tenancy on the cloud by employing algorithms that have non-linear time complexity, unpredictable execution time, and low execution as they happen to the least researched as depicted in Table 3. This then concludes that security issues in cloud computing must be intensively evaluated.

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. Available: 10.1186/s13677-019-0139-6.

[2] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020, DOI: 10.1109/ACCESS.2020.3009876.

[3] A. Markandey, P. Dhamdher, and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 633-636, DOI: 10.1109/GUCON.2018.8675033.

[4] M. O. Alassafi, R. AlGhamdi, A. Alshdadi, A. Al Abdulwahid and S. T. Bakhsh, "Determining Factors about Cloud Security Adoption Framework in Government Organizations: An Exploratory Study," in IEEE Access, vol. 7, pp. 136822-136835, 2019, DOI: 10.1109/ACCESS.2019.2942424.

[5] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, DOI: 10.1109/ACCESS.2021.3054129.

[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 & Security*, vol. 114, p. 102580, 2022. Available: 10.1016/j.cose.2021.102580.

[7] N. Alkhater, R. Walters and G. Wills, "An empirical study of factors influencing cloud adoption among private sector organizations", *Telematics and Informatics*, vol. 35, no. 1, pp. 38-54, 2018. Available: 10.1016/j.tele.2017.09.017.

[8] O. Alfandi, H. Said and S. Khanji, "Analysis of Cloud Computing Attacks and Countermeasures", *Academia.edu*, 2022.

[9] P. T. Dinh and M. Park, "Dynamic Economic-Denial-of-Sustainability (DDoS) Detection in SDN-based Cloud," 2020 Fifth

International Conference on Fog and Mobile Edge Computing (FMEC), 2020, pp. 62-69, DOI: 10.1109/FMEC49853.2020.9144972.

[10] N. Saravanan and A. Umamakeswari, "Lattice-based access control for protecting user data in cloud environments with hybrid security", *Computers & Security*, vol. 100, p. 102074, 2021. Available: 10.1016/j.cose.2020.102074.

[11] S. Liu, K. Yue, H. Yang, L. Liu, X. Duan, and T. Guo, "The Research on SaaS Model Based on Cloud Computing," 2018 2nd IEEE Advanced Information Management, Communicates, Electronic, and Automation Control Conference (IMCEC), 2018, pp. 1959-1962, DOI: 10.1109/IMCEC.2018.8469462.

[12] M. Saraswat and R. C. Tripathi, "Cloud Computing: Analysis of Top 5 CSPs in SaaS, PaaS, and IaaS Platforms," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 300-305, DOI: 10.1109/SMART50582.2020.9337157.

[13] S. Y. Abdel Ghany and H. Mamdouh Hassan, "Get as you Pay Model for IaaS Cloud Computing," 2018 International Conference on Smart Communications and Networking (SmartNets), 2018, pp. 1-6, DOI. 1109/SMARTNETS.2018.8707412.

[14] 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 & Security*, vol. 114, p. 102580, 2022. DOI: 10.1016/j.cose.2021.102580.

[15] 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. Available: 10.1186/s13677-019-0131-1.

[16] C. Li and C. Yang, "A Novice Group Sharing Method for Public Cloud", *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018. Available: 10.1109/cloud.2018.0014.

[17] 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," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1-6, DOI: 10.1109/ICCSDET.2018.8821135.

[18] M. Tajammul and R. Parveen, "To Carve out Private Cloud with Total Functionality," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 831-835, DOI.1109/ICACCCN51052.2020.9362826.

[19] S. Yi, L. Yuhe and W. Yu, "Cloud Computing Architecture Design of Database Resource Pool Based on Cloud Computing," 2018 International Conference on Information Systems and Computer Aided Education (ICISCAE), 2018, pp. 180-183, DOI: 10.1109/ICISCAE.2018.8666897.

[20] S. Sok, C. Plewnia, S. Tanachutiwat, and H. Lichter, "Optimization of Compute Costs in Hybrid Clouds with Full Rescheduling," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 35-40, DOI: 10.1109/SmartCloud49737.2020.00016.

[21] D. S. Linthicum, "Emerging Hybrid Cloud Patterns," in IEEE Cloud Computing, vol. 3, no. 1, pp. 88-91, 2016, DOI: 10.1109/MCC.2016.22.

[22] 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. Available: 10.1016/j.future.2017.12.017.

[23] S. Bruque-Cámara, J. Moyano-Fuentes an,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. DOI: 10.1016/j.pursup.2016.04.003.

[24] 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," in IEEE Access, vol. 7, pp. 159535-159546, 2019, DOI: 10.1109/ACCESS.2019.2950110.

[25] M. Joshi, S. Budhani, N. Tewari and S. Prakash, "Analytical Review of Data Security in Cloud Computing," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 362-366, DOI: 10.1109/ICIEM51511.2021.9445355.

[26] W. Isharufe, F. Jaafar and S. Butakov, "Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1-6, DOI: 10.1109/ICECCE49384.2020.9179414.

[27]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. DOI: 10.26438/ijsrcse/v5i6.2732.

[28] I. K. Sahu and M. J. Nene, "Model for IaaS Security Model: MISP Framework," 2021 International Conference on Intelligent Technologies (CONIT), 2021, pp. 1-6, DOI: 10.1109/CONIT51480.2021.9498375.

[29] S. Sultan, I. Ahmad, and T. Dimitriou, "Container Security: Issues, Challenges, and the Road Ahead," in IEEE Access, vol. 7, pp. 52976-52996, 2019, DOI: 10.1109/ACCESS.2019.2911732.

[30] K. Timraz, T. Barhoom, and T. Fatayer, "A Confidentiality Scheme for Storing Encrypted Data through Cloud," 2019 IEEE 7th Palestinian International Conference on Electrical and Computer Engineering (PICECE), 2019, pp. 1-5, DOI: 10.1109/PICECE.2019.8747193.

[31] 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. DOI: 10.1109/tetc.2015.2445101.

[32] S. Gokulakrishnan and J. M. Gnanasekar, "Data Integrity and Recovery Management in Cloud Systems," 2020 Fourth International Conference on Inventive Systems and Control (ICISC), 2020, pp. 645-648, DOI: 10.1109/ICISC47916.2020.9171066.

[33] N. A. Patel, "A Survey on Security Techniques used for Confidentiality in Cloud Computing," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1-6, DOI: 10.1109/ICCSDET.2018.8821135.

[34] K. Cheng et al., "Secure kk-NN Query on Encrypted Cloud Data with Multiple Keys," in IEEE Transactions on Big Data, vol. 7, no. 4, pp. 689-702, DOI: 10.1109/TBDATA.2017.2707552.

[35] 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," in IEEE Access, vol. 9, pp. 57792-57807, 2021, DOI: 10.1109/ACCESS.2021.3073203.

[36] P. J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," in IEEE Access, vol. 7, pp. 147420-147452, 2019, DOI: 10.1109/ACCESS.2019.2946185.

[37] S. Chenthara, K. Ahmed, H. Wang and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," in IEEE Access, vol. 7, pp. 74361-74382, 2019, DOI: 10.1109/ACCESS.2019.2919982.

[38] P. Yang, N. Xiong and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," in IEEE Access, vol. 8, pp. 131723-131740, 2020, DOI: 10.1109/ACCESS.2020.3009876.

[39] S. Basu et al., "Cloud computing security challenges & solutions-A survey," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018, pp. 347-356, DOI: 10.1109/CCWC.2018.8301700.

[40] H. Tabrizchi, M. Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions. *Journal of Supercomputing*. 2020, 9493–9532, DOI: 10.1007/s11227-020-03213-1.

[41] 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. DOI: 10.1016/j.jnca.2016.09.002.

[42] D. Malviya and U. Lilhore, "Survey on Security Threats in Cloud Computing", *International Journal of Trend in Scientific Research and Development*, vol. -3, no. -1, pp. 1222-1226, 2018. DOI: 10.31142/ijtsrd19172.

[43] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," 2017 IEEE International Conference on Circuits and Systems (ICCS), 2017, pp. 76-81, DOI: 10.1109/ICCS1.2017.8325966.

[44] S. Pavithra, S. Ramya and S. Prathibha, "A Survey on Cloud Security Issues And Challenges," 2019 3rd International

Conference on Computing and Communications Technologies (ICCCT), 2019, pp. 136-140, DOI: 10.1109/ICCCT2.2019.8824891.

[45] K. N. Sevis and E. Seker, "Survey on Data Integrity in Cloud," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 167-175. DOI: 10.1109/CSCloud.2016.35.

[46] T. Saxena and V. Chourey, "A survey paper on cloud security issues and challenges," 2014 Conference on IT in Business, Industry, and Government (CSIBIG), 2014, pp. 1-5, DOI: 10.1109/CSIBIG.2014.7056957.

[47] S. H. Nagesh, K. R. A. Kumar, and K. T. Rajgopal, "Cloud architectures encountering data security and privacy concerns — A review," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 1729-173DOI: 10.1109/ICECDS.2017.8389745.

[48] N. A. Patel, "A Survey on Security Techniques used for Confidentiality in Cloud Computing," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), 2018, pp. 1-6, DOI: 10.1109/ICCSDET.2018.8821135.

[49] T. Mahboob, M. Zahid and G. Ahmad, "Adopting information security techniques for cloud computing—A survey," 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2016, pp. 7-11, DOI: 10.1109/ICITISEE.2016.7803038.

[50] W. C. N. Kaura and A. Lal, "Survey paper on cloud computing security," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1-6, DOI: 10.1109/ICIIECS.2017.8276134.

[51] J. Li, H. Jiang, W. Jiang, J. Wu and W. Du, "SDN-based Stateful Firewall for Cloud," 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), 2020, pp. 157-161, DOI: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00037.

[52] 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 & Technology*, vol. 6, no. 3, pp. 31–35, May 2018, DOI: 10.21276/ijircst.2018.6.3.3.

[53] S. Mansfield-Devine, "Masking sensitive data," *Network Security*, vol. 2014, no. 10, pp. 17–20, DOI: 10.1016/s1353-4858(14)70104-7.

[54] 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, pp. 1–11, DOI: 10.1155/2018/2615249.

[55] H. Wang and J. Zhang, "-Based Data Integrity Verification for Large-Scale IoT Data," in IEEE Access, vol. 7, pp. 164996-165006, 2019, DOI: 10.1109/ACCESS.2019.2952635.

[56] A. Juels and A. Oprea, "New approaches to security and availability for cloud data," *Communications of the ACM*, vol. 56, no. 2, p. 64, Feb. 2013, DOI: 10.1145/2408776.2408793.

[57] S. Kang, B. Veeravalli, K. M. Mi Aung and C. Jin, "An efficient scheme to ensure data availability for a cloud service provider," 2014 IEEE International Conference on Big Data (Big Data), 2014, pp. 15-20, DOI: 10.1109/BigData.2014.7004378.

[58] S. Uthayashangar, T. Dhanya, S. Dharshini, and R. Gayathri, "Decentralized -Based System for Secure Data Storage in Cloud," 2021 International Conference on System, Computation and Automation, and Networking (ICSCAN), 2021, pp. 1-5, DOI: 10.1109/ICSCAN53069.2021.9526408.

[59] M. J. Page *et al.*, "The PRISMA 2020 statement: an Updated Guideline for Reporting Systematic Reviews," *BMJ*, vol. 372, no. 71, p. n71, Mar. 2021, DOI: 10.1136/BMJ.n71.

[60] 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*, Oct. 2020, DOI:10.1016/j.jksuci.2020.10.015.

[61] M. La Manna, L. Treccozzi, 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, DOI: 10.3390/s21020515.

[62] 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, pp. 1–16, DOI: 10.1155/2017/2046735.

[63] 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 & Its Applications*, vol. 6, no. 4, pp. 43–52, DOI: 10.5121/ijnsa.2014.6404.

[64] V. Gudditti and P. Venkata Krishna, "Lightweight encryption model for a map-reduce layer to preserve security in the big data and cloud," *Materials Today: Proceedings*, DOI: 10.1016/j.matpr.2021.01.190.

[65] K. S. Gill, S. Saxena, and A. Sharma, "GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot," *Computers & Security*, vol. 92, p. 101732, DOI: 10.1016/j.cose.2020.101732.

[66] B. Prabhu kavin and S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Computer Networks*, vol. 151, pp. 181–190, DOI: 10.1016/j.comnet.2019.01.032.

[67] F. Amato, F. Moscato, V. Moscato, and F. Colace, "Improving security in the cloud by formal modeling of IaaS resources," *Future Generation Computer Systems*, vol. 87, pp. 754–764, 2018, DOI: 10.1016/j.future.2017.08.016.

[68] P. R, G. Tony Santhosh, I. A. Juben Ratchnayaraj, and E. Jemiline, "The security in the web application of cloud and IoT service," *Materials Today: Proceedings*, Nov. 2020, DOI: 10.1016/j.matpr.2020.10.087.

[69] N. Saravanan and A. Umamakeswari, "Lattice-based access control for protecting user data in cloud environments with hybrid security," *Computers & Security*, vol. 100, p. 102074, DOI: 10.1016/j.cose.2020.102074.

[70] K. Ganga Devi and R. Renuga Devi, "S2OPE security: Shuffle standard onetime padding encryption for improving secured data storage in a decentralized cloud environment," *Materials Today: Proceedings*,2021, DOI: 10.1016/j.matpr.2021.01.254.

[71] Y. Nugraha and A. Martin, "Towards a framework for trustworthy data security level agreement in cloud procurement," *Computers & Security*, p. 102266, 2021, DOI: 10.1016/j.cose.2021.102266.

[72] A. S. Mohammad and M. R. Pradhan, "Machine learning with big data analytics for cloud security," *Computers & Electrical Engineering*, vol. 96, p. 107527,2021, DOI: 10.1016/j.compeleceng.2021.107527.

[73] M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," *International Journal of Information Management*, vol. 36, no. 4, pp. 618–625,2016, DOI: 10.1016/j.ijinfomgt.2016.03.005.

[74] D. G. Pal, "A Novel Open Security Framework for Cloud Computing," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, vol. 1, no. 2, 2012, DOI: 10.11591/closer.v1i2.371.

[75] R. Patil, H. Dudeja, and C. Modi, "Designing an efficient security framework for detecting intrusions in a virtual network of cloud computing," *Computers & Security*, vol. 85, pp. 402–422,2019, DOI: 10.1016/j.cose.2019.05.016.

[76] M. Hawedi, C. Talhi, and H. Boucheneb, "Security as a Service for Public Cloud Tenants(SaaS)," *Procedia Computer Science*, vol. 130, pp. 1025–1030, 2018, doi: 10.1016/j.procs.2018.04.143.

[77] S. Mall and S. K. Saroj, "A New Security Framework for Cloud Data," *Procedia Computer Science*, vol. 143, pp. 765–775, 2018, DOI: 10.1016/j.procs.2018.10.397.

[78] M. Elsayed and M. Zulkernine, "Offering security diagnosis as a service for cloud SaaS applications," *Journal of Information Security and Applications*, vol. 44, pp. 32–48, 2019, DOI: 10.1016/j.jisa.2018.11.006.

[79] H. Jia *et al.*, "Security Strategy for Virtual Machine Allocation in Cloud Computing," *Procedia Computer Science*, vol. 147, pp. 140–144, 2019, DOI: 10.1016/j.procs.2019.01.204.

[80] M. Elsayed and M. Zulkernine, "Offering security diagnosis as a service for cloud SaaS applications," *Journal of Information Security and Applications*, vol. 44, pp. 32–48, 2019, DOI: 10.1016/j.jisa.2018.11.006.

[81] R. R. Corpuz, B. D. Gerardo, and R. P. Medina, "Using a Modified Approach of Blowfish Algorithm for Data Security in Cloud Computing," *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City - ICIT 2018*, 2018, DOI: 10.1145/3301551.3301597.

[82] L. Yang and Z. Wang, "Research and Design of Multi Dimension Protection System for Data Security in Cloud Computing Environment," *2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC)*,2017, DOI: 10.1109/icctec.2017.00086.

[83] F. Kong, Y. Zhou, B. Xia, L. Pan, and L. Zhu, "A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment," *IEEE Access*, pp. 1–1, 2019, DOI: 10.1109/access.2019.2950731.

[84] T. A. Mohammed and A. B. Mohammed, "Security architectures for Sensitive Data in Cloud Computing," *Proceedings of the 6th International Conference on Engineering & MIS 2020*, 2020, DOI: 10.1145/3410352.3410828.

[85] A. Vemulapalli, "risk assessment for big data in cloud computing environment from the perspective of security, privacy, and trust," *journal of mechanics of continua and mathematical sciences*, vol. 15, no. 8, 2020, DOI: 10.26782/jmcms.2020.08.00036.

[86] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security," *Cluster Computing*, 2020, DOI: 10.1007/s10586-020-03157-4.

[87] O. Krieger, "Security in a Cloud Bazaar," *Proceedings of 2021 on Cloud Computing Security Workshop*,2021, DOI: 10.1145/3474123.3486791.

[88] Md. A. Hossain and Md. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *International Journal of Computers and Applications*, pp. 1–10, 2020, DOI: 10.1080/1206212x.2020.1809177.

[89] A. K. Bermani, T. A. K. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 1–12, 2021, DOI: 10.1080/09720529.2020.1859799.

[90] P. Vörös, D. Csubák, P. Hudoba, and A. Kiss, "Securing personal data in the public cloud," *Journal of Information and Telecommunication*, vol. 4, no. 1, pp. 51–66,2019, DOI: 10.1080/24751839.2019.1686684.

[91] S. Srisakthi and G. A. Ansari, "PCSP: A Protected Cloud Storage Provider employing lightweight techniques," *Information Security Journal: A Global Perspective*, pp. 1–12, 2021, DOI: 10.1080/19393555.2021.1900465.

[92] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," *IEEE Cloud Computing*, vol. 2, no. 2, pp. 30–38, 2015, DOI: 10.1109/mcc.2015.45.

[93] N. Agarwal, A. Rana, and J. P. Pandey, "Guarded dual authentication based DRM with resurgence dynamic encryption techniques," *Enterprise Information Systems*, vol. 13, no. 3, pp. 257–280, 2018, DOI: 10.1080/17517575.2018.1527041.

[94] N. Mishra and R. K. Singh, "Prioritisation and security defense algorithm for cloud-specific vulnerability through the scoring and base metric group," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 481–491,2020, DOI: 10.1080/09720502.2020.1731961.

[95] S. P. Kumar, R. Anandan, F. Tchier, G. Rajchakit, C. Park, and F. M. O. Tawfiq, "Secured data storage in the cloud using logical Pk-Anonymization with Map Reduce methods and key generation in cloud computing," *Journal of Taibah University for Science*, vol. 15, no. 1, pp. 746–756, 2021, DOI: 10.1080/16583655.2021.2001938.

[96] J. K. Dawson, F. Twum, J. B. H. Acquah, Y. M. Missah, and B. B. K. Ayawli, "An enhanced RSA algorithm using Gaussian interpolation formula," *International Journal of Computer Aided Engineering and Technology*, vol. 16, no. 4, p. 534, 2022, DOI: 10.1504/ijcaet.2022.123996.

[97] P. Vörös, D. Csubák, P. Hudoba, and A. Kiss, "Securing personal data in the public

cloud," *Journal of Information and Telecommunication*, vol. 4, no. 1, pp. 51–66,2019, DOI: 10.1080/24751839.2019.1686684.

[98] A. Awad, A. Matthews, Y. Qiao, and B. Lee, "Chaotic Searchable Encryption for Mobile Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 440–452, 2018, DOI: 10.1109/tcc.2015.2511747.

[99] M. Kolhar, M. M. Abu-Alhaj, and S. M. Abd El-Atty, "Cloud Data Auditing Techniques with a Focus on Privacy and Security," *IEEE Security & Privacy*, vol. 15, no. 1, pp. 42–51, 2017, DOI: 10.1109/msp.2017.16.

[100] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Dai, "Deployment of Robust Security Scheme in SDN Based 5G Network over NFV Enabled Cloud Environment," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 866–877, 2021, DOI: 10.1109/tetc.2018.2879714.

[101] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, "An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain," *IEEE Access*, vol. 9, pp. 69513–69526, 2021, DOI: 10.1109/access.2021.3077123.

[102] O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," *IEEE Access*, vol. 8, pp. 210855–210867, 2020, DOI: 10.1109/access.2020.3039163.

[103] J. Aikat *et al.*, "Rethinking Security in the Era of Cloud Computing," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 60–69, 2017, DOI: 10.1109/msp.2017.80.

[104] M. C. Sekhar and K. Kethineni, "Secure Data Sharing in Cloud Computing Using Revocable- Storage Identity-Based Encryption," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 7, pp. 1094–1107, 2018, DOI: 10.26438/ijcse/v6i7.10941107.

[105] R. K and H. P. Mohan Kumar, "Block Design Key for Secure Data Sharing in Cloud Computing," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 369–374,2019, DOI: 10.32628/cseit1953107.

[106] P. Jena, A. Tripathy, S. Swagatam, S. Rath, and A. R. Tripathy, "DUAL ENCRYPTION MODEL FOR PRESERVING PRIVACY IN CLOUD COMPUTING," *Advances in Mathematics: Scientific Journal*, vol. 9, no. 9, pp. 6667–6678, 2020, DOI: 10.37418/amsj.9.9.24.

[107] S. Habib Gill *et al.*, "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study," *Intelligent Automation & Soft Computing*, vol. 31, no. 1, pp. 117–128, 2022, DOI: 10.32604/iasc.2022.016597.

[108] P. V. Maitri and A. Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*,2016, DOI: 10.1109/wispnet.2016.7566416.

[109] Mall, S., and Saroj, S. K. (2018). A new security framework for cloud data. *Procedia computer science*, *143*, 765-775.

[110] N. Mishra and R. K. Singh, "Prioritisation and security defense algorithm for cloud-specific vulnerability through the scoring and base metric group," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 481–491, 2020, DOI: 10.1080/09720502.2020.1731961.

[111] P. Sivakumar, M. NandhaKumar, R. Jayaraj, and A. Sakthi. Kumaran, "Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud," *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, 2019, DOI: 10.1109/icscan.2019.8878749.

[112] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," *IEEE Xplore*, 2018. https://ieeexplore.ieee.org/document/8372705

[113] B. M.P and K. R. R. Babu, "Secure cloud storage using AES encryption," *IEEE Xplore*, 2016. https://ieeexplore.ieee.org/abstract/document/7877709.

[114] A. Kumar, V. Jain, and A. Yadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, 2020, DOI: 10.1109/parc49193.2020.236666.

[115] S. Kathiresan and U. V, "ERSA: Enhanced RSA Cryptography Algorithm to Guarantee High-Security Level for Data in Cloud Environment," *International Journal of Computer Aided Engineering and Technology*, vol. 13, no. 1, p. 1, 2021, DOI: 10.1504/ijcaet.2021.10026517.

[116] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," *2017 World Congress on Computing and Communication Technologies (WCCCT)*, 2017, DOI: 10.1109/wccct.2016.50.

[117] T. P. Anithaashri, A. Benjamin. Joseph, and G. Ravichandran, "Enhancing the Cloud Security using Novel Dominant Game Strategy," *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2021, DOI: 10.1109/icirca51532.2021.9544645.

[118] K. Jaspin, S. Selvan, S. Sahana, and G. Thanmai, "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm," *IEEE Xplore*,2021. https://ieeexplore.ieee.org/document/9397005.

[119] H. Qiu, H. Noura, M. Qiu, Z. Ming, and G. Memmi, "A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT," *IEEE Transactions on Cloud Computing*, pp. 1–1, 2019, DOI: 10.1109/TCC.2019.2911679.

[120] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-rimy, "Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges," *Applied Sciences*, vol. 11, no. 19, p. 9005, 2021, DOI: 10.3390/app11199005.

[121] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," *IEEE Transactions on Engineering Management*, pp. 1–18, 2021, DOI: 10.1109/tem.2020.3045661.

[122] P. Anjaneyulu and Mr. S. S. Reddy, "Cloud Computing Adoption Approach towards Securing Data in Cloud Computing," *International Journal of Trend in Scientific Research and Development*, vol. Volume-2, no. Issue-4, pp. 390–393, DOI: 10.31142/ijtsrd12995.

[123] S. Kaushik and C. Gandhi, "Ensure Hierarchal Identity Based Data Security in Cloud Environment," *International Journal of Cloud Applications and Computing*, vol. 9, no. 4, pp. 21–36, 2019, DOI: 10.4018/ijcac.2019100102.

[124] Q. He and H. He, "A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining," *Sustainability*, vol. 13, no. 1, p. 101,2020, DOI: 10.3390/su13010101.

[125] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," *Information Sciences*, vol. 387, pp. 103–115, 2017, DOI: 10.1016/j.ins.2016.09.005.

[126] K. Gai, M. Qiu, and H. Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data," *IEEE Xplore*, 2016. https://ieeexplore.ieee.org/document/7502279

[127] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *International Journal of Intelligent Networks*, vol. 2, pp. 18–33, 2021, DOI: 10.1016/j.ijin.2021.03.001.

[128] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, 2020, DOI: 10.1007/s40860-020-00115-0.

[129] C. Thirumalai, S. Mohan, and G. Srivastava, "An efficient public key secure scheme for cloud and IoT security," *Computer Communications*, vol. 150, pp. 634–643,2020, DOI: 10.1016/j.comcom.2019.12.015.

[130] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Computer Science*, vol. 125, pp. 691–697, 2018, DOI: 10.1016/j.procs.2017.12.089.

[131] S. Parikh, D. Dave, R. Patel, and N. Doshi, "Security and Privacy Issues in Cloud, Fog and Edge Computing," *Procedia Computer Science*, vol. 160, pp. 734–739, 2019, DOI: 10.1016/j.procs.2019.11.018.

[132] M. Albanese, A. De Benedictis, D. D. J. de Macedo, and F. Messina, "Security and trust in cloud application life-cycle management," *Future Generation Computer Systems*, vol. 111, pp. 934–936,2020, DOI: 10.1016/j.future.2020.01.025.

[133] 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, DOI: 10.1080/08874417.2016.1192520.

[134] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 100–110, 2021, DOI: 10.1016/j.gltp.2021.01.014.

[135] H. Wei, G.-Y. Hu, Z.-J. Zhou, P.-L. Qiao, Z.-G. Zhou, and Y.-M. Zhang, "A new BRB model for security-state assessment of cloud computing based on the impact of external and internal environments," *Computers & Security*, vol. 73, pp. 207–218,2018, DOI: 10.1016/j.cose.2017.11.003.

[136] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, and S. F. Abdulkareem, "Iraqi e-government and cloud computing development based on unified citizen identification," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 4, p. 1776,2019, DOI: 10.21533/pen.v7i4.840.