electronics

MDPI

Review

Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey

Abdul Razaque [1,*], Mohamed Ben Haj Frej [2], Bandar Alotaibi [3,4,*] and Munif Alotaibi [5,*]

[1] Department of Cybersecurity, International Information Technology University, Almaty 050000, Kazakhstan;
[2] Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, USA; mhenhaj@bridgeport.edu
[3] Department of Information Technology, University of Tabuk, Tabuk 47731, Saudi Arabia
[4] Sensor Networks and Cellular Systems (SNCS) Research Center, University of Tabuk, Tabuk 47731, Saudi Arabia
[5] Department of Computer Science, Shaqra University, Shaqra 15526, Saudi Arabia
* Correspondence: a.razaque@iitu.edu.kz (A.R.); b-alotaibi@ut.edu.sa (B.A.); munif@su.edu.sa (M.A.)

Abstract: Cloud computing has become a prominent technology due to its important utility service; this service concentrates on outsourcing data to organizations and individual consumers. Cloud computing has considerably changed the manner in which individuals or organizations store, retrieve, and organize their personal information. Despite the manifest development in cloud computing, there are still some concerns regarding the level of security and issues related to adopting cloud computing that prevent users from fully trusting this useful technology. Hence, for the sake of reinforcing the trust between cloud clients (CC) and cloud service providers (CSP), as well as safeguarding the CC's data in the cloud, several security paradigms of cloud computing based on a third-party auditor (TPA) have been introduced. The TPA, as a trusted party, is responsible for checking the integrity of the CC's data and all the critical information associated with it. However, the TPA could become an adversary and could aim to deteriorate the privacy of the CC's data by playing a malicious role. In this paper, we present the state of the art of cloud computing's privacy-preserving models (PPM) based on a TPA. Three TPA factors of paramount significance are discussed: TPA involvement, security requirements, and security threats caused by vulnerabilities. Moreover, TPA's privacy preserving models are comprehensively analyzed and categorized into different classes with an emphasis on their dynamicity. Finally, we discuss the limitations of the models and present our recommendations for their improvement.

Keywords: cloud computing; security; service level agreement; privacy-preserving model; third-party auditor; cloud service provider; cloud client

Citation: Razaque, A.; Frej, M.B.H.; Alotaibi, B.; Alotaibi, M. Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. *Electronics* **2021**, *10*, 2721. https://doi.org/10.3390/electronics10212721

Academic Editor: Dimitra I. Kaklamani

Received: 23 September 2021
Accepted: 28 October 2021
Published: 8 November 2021

1. Introduction

Cloud computing is considered as a utility-driven paradigm derived from a "pay as you use" concept responsible for enabling consumers to remotely share technology-based resources instead of possessing these resources locally [1,2].

Cloud computing transports a reliable, custom-made information technology (IT) perimeter for cloud users with an ensured quality of service. In cloud computing, services are afforded from the cloud clients' points of view and are presented as IT-related skills, reachable with no in-depth familiarity of the used technologies and with a titular coordinating effort [3,4].

The cloud as a concept can be defined as the "storing of data anywhere and accessing it anytime". Cloud clients who have appropriate permissions can access the stored data. For more information about the cloud characteristics, readers can refer to [5]. Four diverse types of delivery models are supported in cloud computing: private cloud, public cloud, hybrid cloud, and community cloud [6,7].

- The private cloud is usually utilized by a limited number of users capable of accessing highly confidential data.
- The public cloud is commonly employed for hosting sensitive data, in which data integrity is repeatedly mutable.
- The hybrid cloud combines two or more delivery models. This model can be applicable to cloud users who would like to retain their most crucial data on-premises while storing their fundamental data on the cloud. The combined delivery models can be private-, public-, or community-based models; however, a standardized technology can be utilized to bound the data. The hybrid cloud improves security and lowers the price. However, the high management complexity is the major drawback.
- The community cloud can be considered as a type of public cloud in which various cloud clients share a specific infrastructure with a community that engages with one another on an identical interest.

Cloud computing merges various technologies and procedures to preserve cloud client's data. Thus, there are competitions between cloud service providers to provide the latest security mechanisms. Notwithstanding, several security-wise ambiguities still exist which make many organizations reluctant to fully utilize cloud computing [8].

In cloud computing, data security, privacy, and safety are fundamental measures which establish the trust level between the cloud clients and cloud providers. Cloud computing is broadly employed in diverse fields such as economy, social, finance, educational institutions, and government offices. Therefore, users store confidential information on the cloud and retrieve it at their convenience. Prior to developing and designing cloud computing, privacy and security requirements have to be exhaustively explored. Individuals and organizations are still distrustful due to the existing security vulnerabilities that threaten cloud computing. In fact, cloud computing lacks explicit security and privacy protection regulations.

Several researchers concentrate on recognizing the privacy and security challenges that cloud users encounter. Other researchers investigate the possibility of choosing trustworthy and adequate cloud providers in order to mitigate privacy and security hazards [9]. To deal with privacy and security challenges, the TPA terminology is presented. Cloud clients and cloud providers lack some capabilities which make the TPA (i.e., which has these capabilities) an essential entity in the cloud realm. The TPA can be trusted by both cloud clients and cloud providers to evaluate the security level of cloud service providersÕ storage; thus, the data can be marked as protected against malicious attempts, Byzantine failures, data alteration attacks, and even server colluding attacks [10]. Dynamic TPA-driven approaches provide the data verification and operation, which improve the storage accuracy, dynamic data support, fast localization of the data error, dependability, and lightweight characteristics. The TPA dynamicity involves four steps: revise, erase, append, and then update the operation (depicted in Figure 1).

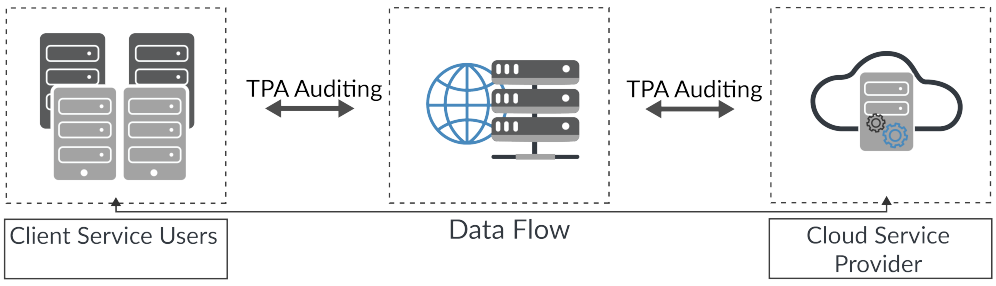

Figure 1. Auditing process based on a TPA.

Cloud security deficiencies are the major factors that prevent several organizations from fully adopting cloud computing. Utilizing a TPA might enhance the companies' desire to hasten the adoption of cloud computing. Nevertheless, TPAs suffer from various

issues. This survey investigates TPA privacy-preserving models' characteristics and the security issues that TPAs suffer from.

1.1. Research Contribution

The contributions of our survey paper can be summarized as:

- The state-of-the-art privacy-preserving TPA-based models for cloud computing are extensively discussed. In addition, these TPA-based models are categorized based on unique characteristics.
- The expected vulnerabilities of cloud computing are comprehensively discussed as they are used by the TPA to launch the threats for violating data privacy.
- TPA-based privacy-preserving security challenges are discussed, and recommendations are suggested either to control or mitigate the malicious intent of the TPA in the cloud computing environment.

1.2. Paper Organization

The remainder of the paper is summarized as follows: Section 2 presents the research methodology. Section 3 discusses related reviews and surveys. Section 4 discusses vulnerabilities and potential threats. We summarize and recapitulate all the studied methods in Section 5. Section 6 discusses the TPA-based security challenges and recommendations. Finally, Section 7 concludes our survey.

2. Research Methodology

An integrative evaluation scheme is employed for survey organizations. This survey aims to focus on the privacy-preserving models in cloud computing based on a third-party auditor and cloud vulnerabilities. For example, what types of privacy-preserving models are more compatible for blocking the malicious role of the TPA? What are the security requirements for maintaining data privacy? What are the vulnerabilities that help the TPA to deteriorate data privacy and thus lead to security threats? What vulnerabilities should be addressed to improve the performance of cloud computing from the privacy-preserving perspective? Because data privacy is of paramount significance, negligence in privacy can reduce users' confidence in cloud computing. A qualitative study is used to find the answers to these state-of-the-art questions. The qualitative study helps to collect ground-breaking information regarding the privacy-preserving models to avoid being a victim of the TPA. However, the assessment method of conducting the survey is not entirely systematic, and the assessments attempt to cover completely blinded and peer-reviewed scholarly articles on privacy preservation. These articles are focused on the years 2010–2021. The source of collecting the information is extremely explicit and is based on peer-reviewed research articles, books, conferences, and sources published. These sources comprise various databases (e.g., PubMed, MetaPress, IEEE Digital Library, CINAHL, Trip Database, Science@Direct, ERIC, arXiv e-Print Archive, Social Science Research Network, CORE, Semantic Scholar Directory of Open Access Journals, and ProQuest). These sources support the collection of the articles to discuss the state of the art of cloud computingÕs privacy-preserving models. Different keywords were used to locate the articles, such as the categorization of PPM based on a TPA, the involvement of a TPA for exploiting the data privacy including the security requirements, and the vulnerabilities that lead to security threats from the TPA. The search returned numerous articles, but 64 articles were carefully chosen that were highly related to our review. Ten articles were used to write the introduction section, 11 were related to the existing reviews/surveys on the security of cloud computing, 16 articles were related to the security requirements, vulnerabilities, and threats, and 37 articles were used to describe the recapitulation of TPA studied methods including PPM. These state-of-the-art articles have given deep insights into the vulnerabilities, including the elements of security requirements.

3. Related Reviews/Surveys

In this section, existing state-of-the-art reviews/surveys are discussed. Most of the existing reviews/surveys focused on the field of intrusion detection and prevention systems in cloud computing. For instance, ref. [11] presented a systematic review on intrusion detection and prevention systems (IDPS) and alarm management techniques.

The authors of [12] put forward a comprehensive taxonomy on intrusion detection and prevention systems for cloud computing. In [13], the authors presented the cloud intrusion detection system (IDS) and intrusion detection and prevent system frameworks in a comprehensive review of the challenges of intrusion detection/prevention system in cloud computing. In [14], the authors suggested a taxonomy on the open-research issues in the field of intrusion detection systems that use computational intelligence (CI) methods in a (mobile) cloud environment. The authors of [15] presented a review of cloud-based intrusion detection systems concerning their various types, positioning, detection time, detection techniques, data source, and attacks. Other articles focused on the infrastructure as a service (IaaS) model, where multitenancy is an option to reduce the cost of hosting. In [16], the authors put forward a review on the current issues that could emerge from multitenancy and then proposed solutions to mitigate them. In [17], the authors presented a survey on the impact of multitenancy when it comes to cloud forensics challenges and solutions. In [18], the authors suggested a systematic review of scheduling approaches on multitenancy scheduling approaches in cloud platforms. In [19], the authors presented a loophole in data security in cloud computing when a guest OS is run over a hypervisor without knowing the reliability of the guest OS. The authors of [20] brought forward a survey consisting of the classification of the state-of-the-art methods on data replication schemes and their open issues.

The authors of [21] surveyed the methods, products, and challenges and reviewed the masking practices for outsourced data based on data splitting and anonymization, in addition to cryptographic techniques covered in other surveys. In [22], the authors presented a survey focusing on privacy-preserving approaches in cloud computing, such as writing the policies, permissions, access rights, and additionally fragmenting and reconstructing data and anonymizing data. Our proposed survey particularly focuses on the privacy-preserving models for avoiding malicious actions from TPAs. As shown in Table 1, various review papers discussed different aspects of security in cloud computing.

Table 1. Summary of the contributions of existing surveys/reviews.

Existing Reviews/ Survey	Summary	Scope and Focus
[11–15]	Review of intrusion detection and prevention systems (IDPS) in cloud computing	These papers cover the intrusion detection and prevention systems (IDPS)
[16–18]	Review of the cloud vulnerabilities from the multitenancy perspective	The authors mainly cover multitenancy threats
[19,20]	Comprehensive reviews are conducted on the data security from the cloud computing perspective.	The authors cover data security
[21,22]	Privacy preserving models and protocols are surveyed in the cloud computing	These papers cover privacy-preserving in cloud computing
Our proposed survey	This survey presents the privacy-preservation-focused TPA approaches, vulnerabilities, and potential threats in the cloud computing environment	Focus on cloud computing adopting a third-party auditor

4. Vulnerabilities, and Potential Threats

4.1. TPA-Based Cloud Vulnerabilities

Encrypting data on the cloud is necessary while avoiding considerable processing overhead. Many organizations are leaning towards cloud-based IT solutions because of the multiple benefits that cloud computing affords. Nevertheless, before making use of cloud

computing, cloud clients should be aware of potential vulnerabilities (Figure 2) that might mutate cloud clients' hopes of increasing scalability and decreasing coordination cost into a misery of misuse and data breaches [23]. Therefore, the security issues associated with cloud adoption should be considered. The most common vulnerabilities effecting TPAs are given as follows:

- Loss of control;
- Lack of trust (mechanisms).

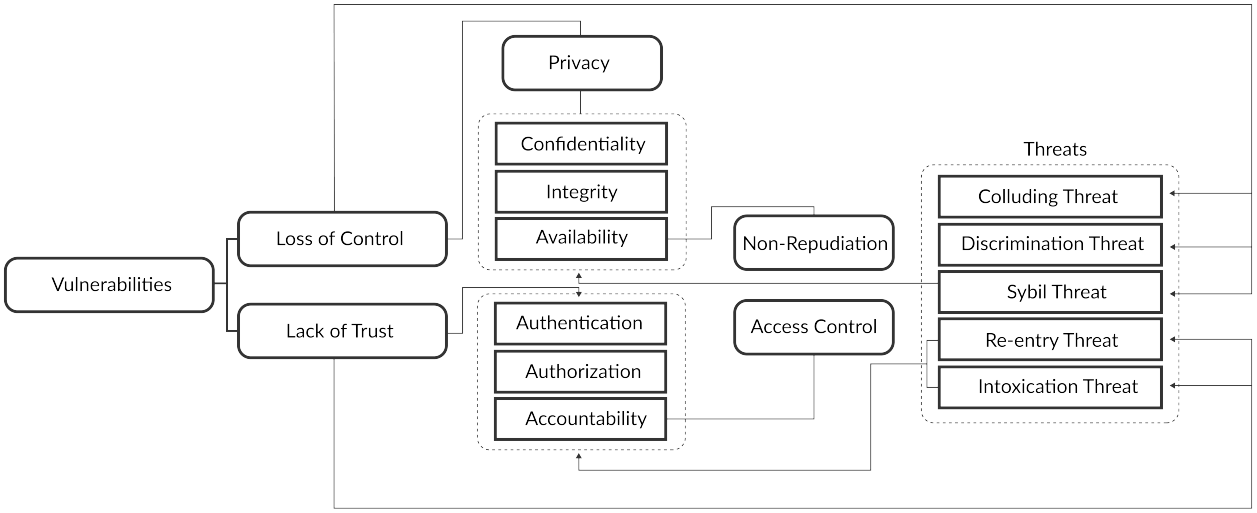

Figure 2. Security requirements, vulnerabilities, and threats.

4.1.1. Loss of Control

When clients/users lose their authority over their resources stored on the servers of the cloud service provider (CSP), a loss of control occurs [24]. A deficiency in authentication and authorization placed by the service providers contributes to bigger security risks and concerns. Most of the cloud services providers do not provide data encryption for the data at rest. As a result, the data cannot be safeguarded if a data breach occurs at the cloud service provider side [25].

Let us consider the server S_c in the CSP and clients $C = \{C_1, C_2, \ldots, C_k\}$ that use the services $S = \{S_1, S_2, \ldots, S_k\}$. We take the security requirements $R_{se} = \{R_{se1}, R_{se2}, \ldots, R_{se-n}\}$ to impose on the server. Thus, the risk $R_{p,q}$ can be referred to as $R_{p,q}$, for $1 \leq p \leq k$ and $1 \leq q \leq n$ that has a security requirements S_p for the clients. We let PS_q, for $1 \leq q \leq n$, be the probability that the server loses the control to meet the security requirements. The loss of control $\forall\gamma$ be determined as:

$$\forall\gamma = \sum_{1 \leq q \leq n} R_{p,q} \times PS_q \tag{1}$$

4.1.2. Lack of Trust (Mechanisms)

Trust is one of the important aspects for maintaining quality. Trust is faith or confidence in the cloud services delivered by the CSP [26]. Trust permits the clients to use the service in the cloud without any panic.

To reinforce the confidence of the clients, it is necessary to build trust among clients, TPA, and CSP. The problem is a lack of trust for data storage on the servers of the clouds for clients. Furthermore, most organizations store their private and sensitive information on cloud servers. If a CSP reliably provides the services, then there is the possibility that a TPA might play a role as a malicious adversary when auditing the services. There is the possibility that the TPA might share the private and sensitive data to other unknown parties to harm the legitimate owners of the data. Thus, there is a need to build a trust model to deal with the lack of trust of the clients. The trust model based on time factor is

considered as feedback. If the feedback is older, it is considered to be of a lower weight, whereas newer feedback is counted as having a higher weight. Thus, the feedback of the client can be determined as:

$$C_{fe} = \frac{1}{1 + \omega(t - T_\delta)} 0 < \sigma \tag{2}$$

where ω is used for the faster time decay, δ is the feedback received from the clients, t is the time during which feedback received from the clients, T is the time during which the CSP gives the feedback to clients, and σ is the slower time decay.

TPA takes the responsibility to evaluate and authenticate the client while maintaining privacy preservation depicted in Figure 3. This is carried out because the actions taken by the TPA could be malicious for the client and CSP.

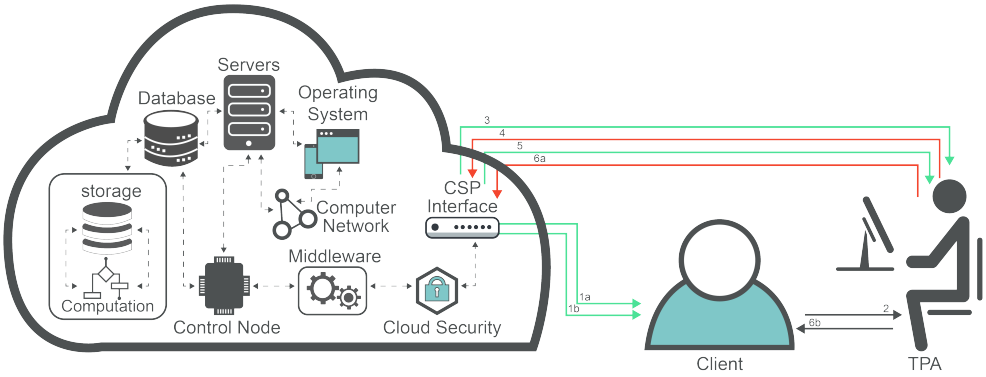

Figure 3. Evaluation and authentication of the client through CPS.

Cloud clients should be aware of the following seven issues.

- Privileged user access;
- Regulatory compliance;
- Data location;
- Data segregation;
- Recovery;
- Investigative support;
- Long-term viability.

4.2. TPA-Based Cloud Threats

Several security requirements are violated because of the diverse attacks that target cloud computing as depicted in Figure 2.

4.2.1. Collusion Threats

This type of threat consist of a form of attack known as collusive malicious feedback that is created by malicious cloud clients who misuse feedbacks to tamper with trust model outcomes. Collusion attacks exist in three forms:

- Self-promoting: malicious cloud clients falsely promote a specific cloud service provider by recording remarkable positive feedback;
- Slandering: malicious cloud clients defame a specific cloud service provider by sending remarkable negative feedback;
- Occasional collusion feedback attack: this kind of attack occurs when a remarkable negative or positive feedback is occasionally entered by malicious cloud clients.

4.2.2. Sybil Threats

This type of attack is launched by malicious cloud clients utilizing several identities to tamper with test outcomes. Various counterfeit ratings are generated by malicious cloud

clients utilizing low product value in which products are purchased in short time. This type of attack can be categorized as:

- Self-promoting: this is also known as a ballot-stuffing attack. In this attack, significant positive feedback is added by malicious cloud clients to promote a specific cloud service provider;
- Slandering: another name of this attack is bad-mouthing. This attack is launched by malicious cloud clients to defame a specific cloud service provider using significant negative ratings.
- Occasional Sybil feedback attack: in this attack, significant amounts of negative or positive feedback are entered occasionally by malicious cloud client to either promote or defame a specific cloud service provider.

4.2.3. ON OFF Threat or Intoxication Threat

Malicious cloud clients adjust their behaviors either to act as harmful or harmless users. More specifically, the cloud client initially performs ordinarily until gaining trust, then the client begins to misbehave. Regrettably, this type of misbehavior is hard to detect. This deficiency is derived from peer-to-peer network and is known as the dynamic personality of peers. This attack can be resolved using a forgetting factor approach.

4.2.4. Discrimination Threat

Discrimination attacks occur when distinct qualities of services are afforded from cloud service providers to cloud clients. This attack jeopardizes cloud service providers' trust because various ratings are provided by clients as a result of this attack. Mitigating or preventing this attack is a difficult task to accomplish.

4.2.5. Newcomer or Reentry Threat

This attack is carried out by a previous client who has been terminated due to unethical behavior and who reenters the domain with a new identification. Reentry or newcomer attack can be mitigated/prevented by contrasting credential records utilizing the client location and then using the location as a unique ID.

5. Recapitulation of TPA Studied Methods

5.1. Privacy-Preserving Model (PPM)

These models as indicated in Table 2 are paramount for protecting the privacy of the data and information.

5.1.1. Security and Privacy For Storage

Wei et al. [27] proposed a protocol to protect and audit the integrity of cloud data. The authors improved the RSA algorithm to audit client's data and avoid revealing data contents. This protocol supports data dynamics operations, including: deletion, modification, and insertion. The proposed approach consists of three components: cloud clients, TPA, and cloud service providers. The cloud clients might have a considerable amount of data that can be stored and retrieved; the cloud service providers can store clients' data and provide the data when clients want to retrieve it at a low-cost price; and the TPA is skillful in affording efficient and unbiased auditing. Generally speaking, cloud service providers should not be trusted. Therefore, CSPs can be trusted through TPAs' services. However, cloud clients must be cautioned when they share their sensitive information with a coexisting TPA. The authors propose the following five algorithms to encrypt the data using RSA and then to apply the auditing mechanism:

- "KeyGenÓ: this algorithm is utilized by the cloud client to generate the public key encryption pair (i.e., the public key and the private key);
- ÒOutsourceÓ: this algorithm is also employed by the cloud client to transfer the data to the CSP;

- ÒAuditÓ: this algorithm is utilized by the TPA to transmit the audited query to the CSP;
- ÒProveÓ: this algorithm is employed by the CSP once the audit query is received from the TPA. Subsequently, the CSP uses the stored data to generate a proof;
- ÒVerifyÓ: this algorithm is utilized by the TPA once the proof is received. The purpose of this algorithm is to check if the proof is correct and not using the public key.

The performance of the proposed protocol is evaluated using two metrics: the computation and the communication costs. At the CSP, the computation cost is calculated through measuring the time that the protocol needs to prove the processed data. This measurement takes into consideration three components: the block size, the length of the audit query, and the time interval of authentication information. On the other hand, the communication cost measures the interplay between the TPA and the CSP. The element used to measure this interaction is the proof transmitted from the CSP to the TPA.

Table 2. Recapitulation based on the key schemes .

Method	KEY-GEN	SIG-GEN	GEN-PROOF	Verify-PROOF	Homomorphic Linear Authenticator	Bilinear Signature	Symmetric Key	Data Security	Generating Signature
SPS [27]	✓		✓	✓					
PPPAS [28]	✓	✓	✓	✓					
PPA [29]	✓	✓	✓	✓	✓				
SEPPPA [30]	✓	✓	✓	✓					
DPVPPM [31]								✓	
EPASS [32]	✓	✓			✓	✓			
RSASS [33]									✓
TSAS [34]						✓			
ESTTP [35]							✓		

5.1.2. PANDA Public Auditing (PPA)

Wang et al. [29] proposed a public auditing approach to secure data storage using a TPA and a modern ciphertext. The proposed approach utilized modern cipher cryptography instead of the encryption to enable secure communication between cloud clients and TPAs. This approach provides two services: storage and data integrity.

In this approach, the outsourced data do not have to be copied by the TPA to perform audits. This method also includes five algorithms. Outsourcing data occurs at the cloud client by encrypting the new ciphertext. Subsequently, the auditing procedure utilizes the following five algorithms:

- ”KeyGen”: the purpose of this algorithm is to generate keys for the cloud client and the TPA;
- “SigGen”: this algorithm is utilized by the TPA to generate the verification metadata;
- “GenProof”: the cloud service provider uses this algorithm to inspect the storage correctness of data and to generate the data state’s proof;
- “VerifyProof”: this algorithm is utilized by the TPA to verify the evidence correctness provided by the CSP.

The following steps clarify how the proposed algorithms are implemented. The owner key is created after encryption by the cloud client utilizing the “KeyGen” algorithm. Subsequently, the cloud client transmits the key along with the processed data via a private channel. On the other hand, the TPA utilizes the “KeyGen” algorithm to generate the challenge key and the “SigGen” algorithm to verify the key. Then, the processed data are encrypted by the TPA to create the crypto-metadata; these metadata are eventually transmitted to the CSP.

For auditing purposes, a challenge is transmitted by the TPA to the CSP utilizing the challenge key. Thereafter, an audit key is created utilizing the “GenProof” algorithm and transmitted to the TPA. Once the audit key is received by the TPA, the TPA uses the “VerifyProof” algorithm to verify the key’s validity in comparison to the verification key, in order to verify the stored data’s integrity.

The authors evaluated their proposed method performance using three metrics: storage, computation costs, and communication costs. The proposed approach achieved low

complexity compared with other related approaches because it adopted a light symmetric encryption algorithm, known as an advanced encryption standard (AES), on a bilinear map. The authors proved that their approach can have shorter auditing requests than the communication lengths that appeared in other related works based on bilinear maps. The storage cost has been also evaluated in comparison to the costs of other related work utilizing bilinear maps; its efficiency in terms of storage costs was thereby proven.

5.1.3. Privacy-Preserving Public Auditing (PPPAS)

Hussien et al. [28] proposed a privacy-preserving public auditing approach to secure cloud storage. This approach is considered the pioneer of public auditing because it is one of the oldest methods that is implemented to preserve data privacy using this type of auditing. The authors also introduced an approach based on homomorphic linear authenticator (HLA) for data privacy-preserving. The HLA utilizes keys to audit using arbitrary masking.

Another privacy-preserving auditing approach is proposed by Anbuchelian et al. [36]. The purpose of this method is to ensure that the TPA is denied from accessing the contents of the audited data. The authors evaluated the performance of the proposed approach and found that the proposed approach is an ideal solution for privacy preservation.

5.1.4. Secure and Efficient Privacy-Preserving Public Auditing (SEPPPA) Protocol

An auditing approach that depends on the TPA audit alone (i.e., with no need to use all of the data) was presented by Pavithra et al. [30]. This approach utilizes batches for auditing and for preserving privacy and integrity. The authors utilized the bilinear map for data encryption [37]. The proposed protocol employs four algorithms: "KeyGen", ÒSigGenÓ, ÒProofGenÓ, and ÒVerifyProofÓ. The "KeyGen" algorithm is used by the cloud client to generate a pair of keys. One is a public key that is obtainable by the auditing entities; however, the authorized TPAs are the only parties that are allowed to use it for auditing. In the second, a private key is generated for the cloud client. The ÒSigGenÓ algorithm is utilized to generate signatures for the outsourced files. The ÒProofGenÓ algorithm is employed by the CSP to generate integrity proof after receiving the challenge [38]. The ÒVerifyProofÓ algorithm is used by the TPA to verify data integrity by utilizing the public key of the CSP. The proposed approach is evaluated by measuring the computation and communication overhead. To evaluate the message exchange complexity of the proposed method, the authors took into consideration three main factors: challenge-response auditing, data outsourcing, and data retrieval [39]. It is known that both the retrieval and outsourcing overhead is unavoidable; therefore, the authors concentrated on the challenge-response overhead. Thus, it was deduced that the complexity of the system is constant [40].

5.1.5. Privacy-Preserving Public Auditing for Shared Cloud Data

Kundu et al. [41] also introduced an approach that can be performed by the TPA to audit the shared data integrity. Data can be audited with no need to store all of the data in the cloud. This method prevents the public verifier from revealing the private identity information of the group member.

To evaluate the performance, the authors measured both the public auditing and dynamic groups. In the dynamic groups, the original user is the responsible party of distributing the private key to new users. Once a specific user is revoked, a re-signing mechanism takes place to avoid downloading all of the shared data again by the revoked user. In active groups, the signers' identities are protected, and the data integrity is audited publicly. The private key is shared securely to group members using dynamic broadcasts capable of encryption. New users can be added to the group, whereas revoking a user requires proxy signatures. This approach forces the TPA to consume more time and bandwidth in order to accomplish a low error detection rate. The major characteristic of this approach is its high-dynamic group efficiency.

Wang et al. [42] proposed a method that helps the TPA to perform various auditing tasks. This method is based on a bilinear aggregate signature. One advantage of this approach is its ability to cope with data dynamic remote integrity check. Another advantage is its capability of carrying out various tasks of public auditing simultaneously. The proposed approach handles multiclient data batch auditing with the help of the BLS signature technique and the Merkle hash tree algorithm. This method provides a valid settlement that facilitates public auditability and enables data dynamics. The keys are produced, and proof is verified by the TPA for both the server and client sides.

5.1.6. Comments on Privacy-Preserving Public Auditing Mechanisms for Shared Cloud Data

Wang [43] discussed the possibility of forgery attacks and data corruption attacks, and in a follow-up work, Wu et al. [44] discussed methods to overcome these issues. The auditing proof contains a set of identifiers which the TPA fails to confirm with the user. As a result, false verification is possible. Fake auditing is also possible from an active adversary utilizing data corruption and generating false auditing to pass verification. To avoid these vulnerabilities, additional steps are added, and the mechanism is modified. These steps involve the setup phase, signing phase, proof generation, and proof verification. This paper also shows the performance analysis to compare their results with the original scheme.

5.1.7. Third Party Auditor: A Potential Solution for Securing a Cloud Environment

Wu et al. [44] presented a technique to recognize malicious insiders in cloud computing. Another feature of the proposed method is its ability to prevent or mitigate various cloud computing attacks. The authors evaluated their proposed solution using a successful prevention rate of malicious access attempts.

5.1.8. Privacy-Preserving Model: A New Scheme for Auditing Cloud Stakeholders

This scheme aims to ensure the privacy and security of the TPA. A study by Wu et al. [44] discussed the potential vulnerabilities of a triangle authentication process by analyzing the data privacy issues and providing a solution to eliminate the threats. The PPM model was developed to audit the stakeholders in the cloud. An experiment was performed to show a malicious insider in TPA and the authentication process in the cloud service provider. The main parameters observed were the effectiveness, operational efficiency, successful rate, and reliability of CSP. This method protects the user's outsourced data in the cloud [45].

5.1.9. Cloud Data Integrity Using a Designated Public Verifier

A public verifier is presented by Razaque et al. [31] to examine the auditing process and to assure confidentiality and data integrity. The proposed approach composed of three components: cloud service provider, cloud service user, and public verifier. Computation services are derived from requirements of users and carried out by cloud service providers. Furthermore, end-to-end communication is executed utilizing secure socket layers to protect data privacy. Moreover, the proposed approach performs privacy-preserving for auditing purposes. The only issue with this approach is the reduction of the TPA efficiency when the number of users increases. The reason for this reduction is the increase in malicious users when the TPA carries out auditing.

5.1.10. Based on Homomorphic Nonlinear Authenticator

The authors of [46] introduced a data possession scheme to verify data integrity in cloud storage. The proposed approach established a homomorphic authenticator using an attribute-based signature. Three parties are involved in this approach; namely, the cloud storage server, the cloud client, and the TPA. This approach relies on a verifier-independent and stateless cloud storage server. Some privacy strategy is implicitly contained within the homomorphic authenticator. Nobody can check data integrity until the attributed strategy

is satisfied by that person. The data owner can generate a delegation key but generating that key fails in subsequent tasks. The party responsible for verifying the data is the TPA if the public key is available; however, in that case, the server is untrusted [47]. Access to applications on the server can be granted by digital signatures granted by a cyclic-group system. This approach provides perfect resistance and vigorous anonymity. However, there still lies an issue with this approach; namely, the data of clients are still at risk if the TPA is not trustworthy [48].

5.1.11. Based on the Proxy Re-Signature Scheme

Erway et al. [49] presented a technique to protect cloud storage and to conceal users' data from the TPA. This approach relies on random masking and a homomorphic nonlinear authenticator to prevent TPAs from learning any users' data while auditing. Nonlinear blocks are used to implement random masking; this mechanism is then sent to clients in the server's response. For that reason, it is impossible for the TPA to reveal the user's data. Shrinivas et al. [32] presented a similar approach for public auditing. This method provides various services: storage consistency, public auditing, batch auditing, and privacy preservation. The following three algorithms were introduced to validate the proposed approach:

- Token precomputation is the aim of the first algorithm;
- To measure accuracy, location errors, and verification, the second algorithm is presented;
- Error recovery is achieved with the help of the third algorithm.

To check storage correctness and privacy preserving, it is required to provide consistent security throughout batch auditing.

To reduce the computation overhead caused by a large number of users when data authenticators are generated, a cloud-based auditing scheme is proposed by Wang et al. [50]. A third-party medium is utilized to perform the operations, and the privacy of that medium is protected by using simple operations. The scheme consists of six steps, which are: algorithm Setup, DataBlind, AuthGen, AuthVerify, Recovery and ProofGen, and ProofVerify. The performance analysis is performed based on computation overhead and computation complexity. Data privacy protection is achieved with this scheme only for acceptable communication overhead. This scheme also sets an expiration period for each authentication to protect privacy.

5.2. Elaborated Key Exchange Algorithm Based on RSA

5.2.1. RSA Based Storage Security

This method is composed of two stages [33]: the first is the integrity stage, while the second is the setup stage. Security is constantly monitored. This technique relies primarily on the PDP for accomplishing storage correctness. With the help of this method, the misbehaving servers are identified, and the dynamic operations are achieved. Variable and large file sizes can be attached with a signature signed by this method. In addition, the shared data integrity is regularly checked to verify the possession of the files. This approach operations can be carried out in real time. Moreover, this method can significantly improve the security of data storage.

5.2.2. Novel Third Party Auditor Scheme

This method consists of two phases [51]; the first relates to the communication between the cloud client and the server, and the second phase relates to the communication between the cloud server and the organization server.

The data files are stored at the cloud server upon the user's request. Unique keys are generated and stored from the data files, and the keys are then sent to the end-user. Subsequently, cloud clients reformat and encrypt the data utilizing the secret key and send them to the server. Once the data file is received, the cloud client unique identification would be retrieved by the storage server.

The second stage (i.e., regarding the communication between the cloud server and the organization server) consists of the following phases:

- System setup: this phase facilitates both the cloud server and the organization server to identify each other. Thereafter, unique identifiers are given to storage servers, which prove their identities in the cloud.
- Key or information exchanges: in case some information is updated in any server, this server should send the update to the other servers in the cloud. This is also the case when an update of the keys occurred in the cloud server, and the cloud server must inform the organization's server.

5.3. Based on Diffie-Hellman

Data Privacy by Authenticating and Secret Sharing (PASS)

Secret sharing is utilized to protect data privacy and security. This mechanism uses public key cryptography to provide cloud data with both privacy and authentication. This approach increases the cost of transmission and avoids storing the secret key. The secret key is protected except if the client's device is compromised. To deal with this challenge, a secure cloud computing mechanism based on symmetric bivariate polynomial-based secret sharing and Elliptical curve Diffie-Hellman (ECDH) can be developed.

- Symmetric bivariate polynomial-based sharing: two types of sharing are supported, a symmetric-based sharing and an asymmetric-based sharing. Therefore, to develop secure cloud computing, symmetric bivariate-base sharing is adopted to use informative feature symmetric properties.
- Elliptic curve Diffie-Hellman (ECDH): this protocol is used because it has most of the capabilities that the elliptic cure discrete algorithm has and is less complex than the multiplicative group algorithm.

The authors proposed two secure cloud computing methods. A trusted third party (TTP) is required in the first method, whereas one is not required in the second method. The second type can be expanded to incorporate multiserve secure cloud computing (MSCC). This type consists of the following three stages for establishing the key: the mutual authentication stage, the key sharing stage, and the key recovery stage. In the first method, the key establishment contains the following two stages: the mutual authentication stage and the key recovery stage. The major advantage of this method is its ability to mutually authenticate clients and servers.

Another advantage of this approach is that it employs the symmetric encryption for the interaction between the client and the cloud server instead of the public key cryptosystem. Thus, the overhead of sharing information between the cloud client and the cloud server is minimal compared to the approaches that rely on public key cryptography. Furthermore, the proposed approach goes through the security analysis and proves its robustness against obtaining the key, even if the client's device is compromised.

5.4. Based on Proof of Retrievability

5.4.1. Proof of Ownership and Retrievability (PoOR) Using Homomorphic Verifiable Tags

Cloud computing has an issue that must be resolved, which is related to duplicate information and the proof of retrieving information in environments in which both the server and client are not fully trustworthy. Yan et al. [52] proposed an approach to address this issue, which was based on proofs of ownership and retrievability (PoOR). The cloud clients can prove they are the owner of the transmitted records with no need to send the documents to the server.

The authors combined three cryptography methods to develop a scalable, secure, and fine-grained access control technique for cloud-outsourced information. The three cryptography methods are proxy re-encryption (PRE), key policy attribute-based encryption (KP-ABE), and lazy re-encryption.

5.4.2. Optimized Proof of Retrievability Scheme

Zheng et al. [53] proposed an approach using two independents cloud servers. The first cloud server is utilized for auditing, and the second cloud server is employed for storage. The capacity of the audit server is decreased. Furthermore, the verification of files saved in cloud storage is accomplished remotely by the audit server. Remote data integrity can be achieved using an efficient verification approach that protects against reset attacks. It is also necessary to impose a massive computation overhead on the cloud client. The proof of retrievability (PoR) approach supports such dynamics.

However, the tags must be computed prior to uploading them. In addition to this, these techniques do not provide a full protection against reset attacks. The reset attack can be triggered at the upload stage by the cloud storage.

The following three distinctive entities form the system architecture:

- Client: an individual or organization that owns data files to transmit to the cloud;
- Cloud storage servers (CSS): the CSP coordinates some entities known as CSSs that utilize cloud audit servers to check integrity;
- Cloud audit server (CAS): when the clients request to access services, the TPA accesses services instead of clients because it has the capabilities and expertise to be trusted.

5.4.3. Secure Certificateless Private Verification (SCLPV)

Certificate-less verification is utilized by [54] to verify cloud clients' storage. The physical paradigm is integrated into the cyber paradigm using the cyber physical system (CPS); thus, elements of these two paradigms can exchange information. Another system, e.g., cyber physical social system (CPSS), includes a social entity associated with it. The proposed approach utilized a proof of retrievability (PoR) method for public verification, which proves its efficiency in proving all the verification tasks successfully.

The major feature of the proposed approach is its ability to prevent malicious auditors. However, the more threats occur, the more the verification overhead increases, and multiple verification methods cannot be properly implemented.

5.5. Based on Erasure Correcting Code

5.5.1. Layered Interleaving Technique

- Third party auditor:
  Delegated data auditing should not be able to lead to the obtaining of clients' data content. The cloud server verification attributes should be sent by the client in an encrypted and secure manner.
- Cloud service provider:
  This entity consists of resources and has a specific expertise in constructing and coordinating distributed cloud storage servers. Cloud computing systems are owned and operated by the CSP. Furthermore, a CSP can lease the cloud computing systems.
- Security analysis:
  Step 1: Creating a challenge token: The client precomputes some verification tokens and sends them to different servers once the file is stored in the cloud. Each server signs the token and transmits it back to the client, so that the client can have a handshaking response for that data that has been stored in the cloud.
  Step 2: Correctness verification: The correctness of distributed storage is not only specified by the response challenge transmitted from the server, but it can also be verified from a secure server.
  Step 3: Data recovery: the data retrieved from the server can be defined as either affected or not affected by malicious users in this step.

5.5.2. Privacy Negotiation Language (PNL) Based on Description Logic

Vigorous cloud services are brought to clients; however, clients' confidential data might still be at risk. Thus, preserving privacy and assuring clients' data correctness are paramount tasks [55]. Some techniques have been introduced to prevent or mitigate security

weaknesses. An approach based on privacy negotiation language (PNL) is proposed to agree upon privacy property between the cloud server and the cloud client. The proposed approach can preserve clients' data privacy and protect it from being illegally distributed by the service provider. A new technique is presented to protect clients from malicious data modification attacks, Byzantine failure, and server colluding attacks. This technique can also ensure users' stored data correctness. The proposed method's iterating frequency is finite; however, it presents an efficient solution and carries out a dynamic data operation.

Providing public auditing is a significant mission to accomplish for stored data in CS. This task can be achieved by utilizing audit reports generated from TPAs. These reports facilitate the evaluation of risks which consumers may encounter when using cloud data services. The reports also help the CSP to guarantee its functionality and to handle security risks.

5.6. Audit and Feedback Scheme

Securing the Cloud Storage Audit Scheme

Some researchers proposed some approaches to address the limitations accompanied with third-party protocols. One of the proposed approaches uses feedback as its main functionality. In some situations, TPAs are considered semitrusted or otherwise potentially malicious parties. Furthermore, not all TPAs are independent and reliable. TPAs and CSPs might conspire to allow the verification and to conceal corrupted incidents in a specific CSP. Zhang et al. [56] introduced a distributed edge differential privacy (DEDP) technique to help clients to check the integrity of stored data themselves instead of relying on TPAs' services. This approach also helps clients to use a feedback-based audit mechanism instead of communicating with the CSP.

The proposed technique composed of the following four stages: set up, release plan, execution plan, and review plan. An aggregate feedback algorithm is employed by the TPA to allow clients to revoke and invoke it. The following aspect should be established when using the feedback-based auditing mechanism: the client can authenticate changes if the TPA modifies the date, owner, or perform the specified computational audit work.

The proposed method can protect the client's data privacy from malicious TPAs. Furthermore, the access of malicious TPAs can be revoked by the client. This method can prevent both frame and collude attacks. This protocol is not computationally expensive, and the client can perform the final verification work. The TPA role is restricted to executing proofs and combining feedback. Executing proofs is required to perform the response concerning computing technique. Furthermore, the processed data are continuously transmitted by the TPA to the server. The authors evaluate the time complexity of their approach to explore the number of sampled blocks that effect the audit plan. The client performs the final verification work.

5.7. Based on Oruta and Knox Approach

5.7.1. Secure Digital Signature Scheme

Three auditing schemes can be vulnerable to active adversary attacks when clients share data in the cloud. These auditing schemes include the distributed storage integrity auditing technique and public auditing specified for nonmanager shared data known as Oruta and Knox. These shortcomings were discussed in [57], and their discussion include the following steps:

- Oruta analysis;
- Knox analysis;
- A security problem solution.

Information stored in the cloud should be protected. Usually, clients store data utilizing internet service providers (ISPs), which is in this situation considered as a third party. The government can easily access client information stored on cloud services that use third party ISPs.

5.7.2. Based on Bilinearity Property

- Third party storage audit service

Cloud servers host the clients' data; the stored data can be remotely retrieved. The retrieval of data by a remote client can expose the service to security challenges. The authors of [34,58] discussed in detail the challenges and clarified the importance of deploying secure and efficient approaches to address these challenges. Subsequently, they used a third-party storage audit service (TSAS) to compare the cloud computing security challenges.

The following properties are of paramount significance and can enable auditing protocols to accomplish the tasks that are designated for:

- Data confidentiality;
- Dynamic auditing;
- Batch auditing.

Furthermore, two important metrics that any auditing protocol should obey are the processing and communication costs. Thus, the trade-off between security and performing tasks in an efficient manner is very significant.

5.7.3. Based on Consensus Assessments Initiative Questionnaire (CAIQ)

- Utilizing third party auditing to manage trust in the cloud:

Zhu et al. [59] presented an approach in order to manage cloud computing trust. This approach utilizes a consensus initiative questionnaire (CAIQ) as its building block. The proposed approach contains various security domains. Each security domain has different security controls that have diverse restrictions. The CAIQ was prepared by the cloud service alliance (CSA).

Once the response is received, a validation process is applied at the top-level security domains (TPSD). Moreover, various security validation (SCV) mechanisms are deployed by TPAs. Mapping takes place between the SCV and TPSD to be able to process the auditing. This technique helps cloud clients select the preferable CSP.

5.7.4. Based on Encryption and Secret Key

- A trusted third party based encryption scheme for ensuring data confidentiality in cloud environment:

The aim of this approach is to create stable encryption key management to enhance the stability of cloud computing. The data are encrypted by the cloud client using symmetric encryption. Additionally, a database of secret keys is preserved by the TTP. The provision of security for cloud computing entities is achieved with the help of shelf protocols.

The TTP module consists of the following four phases: the possession of the secret key, the acquisition of the public key certificates, the exchange of the secret key, and clients' data verification. Once the encryption using this approach takes place, the data confidentiality is guaranteed, and the computational complexity is decreased [35].

Sharma et al. [60] utilized four algorithms to encrypt data in cloud computing to assure cloud data storage security. The used algorithms are: advanced encryption standards (AES), secure hash algorithm-1 (SHA-1), and two-user defined algorithm. AES uses a single key to encrypt and decrypt the data. The used key comes with the following different sizes: 128, 192, and 256 bits. AES is highly secure and computationally inexpensive. This encryption technique has an advantage in which the key has to be shared between the user and the cloud. Thus, the secrecy of the symmetric key might be compromised [61].

SHA-1 is one of well-known cryptographic algorithms used to generate a twenty-byte hash. The length of the message digest produced by SHA-1 is 160 bytes. The algorithm is highly efficient; however, the client has to use a key that matches the specified set of attributes to be able to retrieve the data.

The user-defined algorithms are used to verify correctness and to locate and recover from errors.

5.7.5. Based on a Centralized Approach

- A centralized trust model approach for cloud computing

Kaur et al. [62] introduced a trust model to rate cloud service providers. The authors discussed objective trust versus subjective trust. Subsequently, they proposed to use a third party auditor for cloud service providers rating purposes to provide scores for their services. Furthermore, the end user should provide a feedback in the form of a score to the CSP. Thus, trust is maintained between the cloud client and the CSP.

5.8. Based on Computational Intelligence

- A Three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing:

In this scheme [63], a three-layer storage framework that takes advantage of computational intelligence is proposed. The Hash–Solomon algorithm is designed, which divides the data into several parts. Privacy is preserved by storing a small portion of data in different places; namely the cloud server, fog server, and a local machine. Tests are performed on different sizes of data; encoding and decoding are also carried out for privacy purposes. Theoretical analyses and efficiency analyses are performed to prove that storage efficiency is increased by utilizing this scheme. Privacy is ensured by encoding procedures on each server. Maximum efficiency is achieved with the designed efficiency index [64].

TPA classifications according to requirements is shown in Table 3 and the classifications based on security methods are depicted in Figure 4.

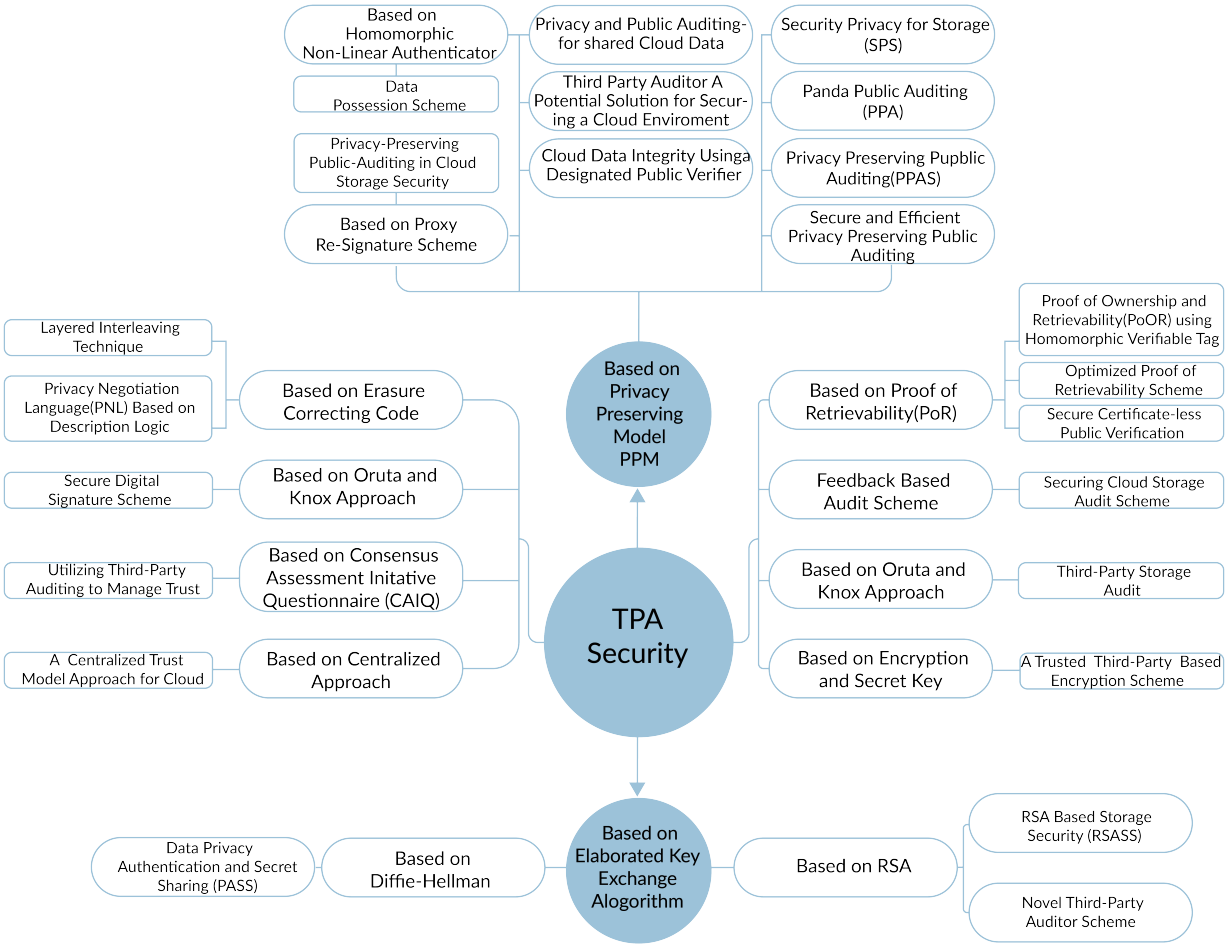

Figure 4. TPA Classification based on the Security Methods.

Table 3. TPA classification by requirements.

Security Model	Security Requirements	Threats	Advantages
SPS [27]	• Third party auditing • Supports data dynamics • Supports privacy-preserving public auditing • Use of private channels to relay information	• TPA somehow trusted • Cost not low enough	• Cost efficient • Practical for cloud systems on large scales • Considers vulnerabilities of dynamic data • Communication overhead
PPA [37]	• Third party auditing • Supports data dynamics • Double block transportation • Supports privacy-preserving public auditing	• TPA used as an intermediary to send encrypted data • Hidden server failure	• Cost efficient • Practical for cloud systems on a large scale • TPA does not need a local copy of data
PPPAS [39]	• Third party auditing • Supports batch auditing • Supports privacy-preserving public auditing	• Relies on TPA	• TPA does not need a local copy of data • Identification of invalid response • Support for dynamic data
SEPPPA [40]	• Third party auditing • Supports batch auditing • Supports privacy-preserving public auditing	• TPA somehow trusted	• TPA does not need a local copy of data • Pioneer in privacy-preserving schemes for cloud
PPPASCD [41]	• The proxy re-signature scheme is used for outsourcing the updated operations • The private key is shared between the group's shared data for computing signatures. • Encryption is conducted by dynamic broadcast; to distribute the private key to the active group members securely	• TPA consumes more time and bandwidth to achieve high error detection probability	• Highly efficient for dynamic groups • Public auditability and data are dynamic for a remote data integrity check
MPPA [43]	• possibility of a forgery attack and data corruption attack • Setup phase, signing phase, proof generation, and verification	• False verification is possible	• Adversary attacks are minimized compared to the original scheme
SCETPA [44]	• An auditing protocol for ensuring the integrity of the third-party auditor using the time-released session keys • It also uses the PPM technique • It ensures integrity using time-bounded session keys	• The public verifier is not trusted	• Malicious insiders and threats are reduced • Data privacy is protected
PPMACS [45]	• Analyze the various vulnerabilities in data stored in the cloud by securing the TPA • Effectiveness, operational efficiency, and reliability are measured	• The malicious insider in TPA	• The effective authentication process for auditing stakeholders
DPVPPM [31]	• Data security scheme is utilized for the public verifier to Audit the data of the cloud user • It uses privacy-preserving model technique • A designated public verifier is a trusted entity such as TPA	• Multiple auditing is not supported	• Efficiency and reliability are much improved • Computational burden is reduced
DPS [46]	• To check the data integrity, an attribute-based signature is utilized to construct a homomorphic authenticator. • cloud storage server is stateless and verifier independent • TPA has the public key, and it acts as a verifier	• Cloud storage server cannot be trusted • TPA should be trustworthy	• Maintains strong anonymity in the cloud environment • Good resistance
PPACSS [49]	• Uses homomorphic nonlinear authenticator, and a random masking technique • Security consistency is required for batch auditing to secure the correctness of the stored data. • The short signature scheme is used for the auditing protocol and the public auditing	• A local copy of the data can be presented in the TPA	• UserÕs outsourced data is secured in the cloud • TPA achieves better efficiency while performing multiple auditing tasks
RSASS [33]	• RSA algorithm is used to generate the signature for handling large data files • It is mainly based on a provable data possession scheme to achieve storage correctness • Security is constantly maintained • Generates signature which can be used for files of large and different size	• TPA has the private key which could be unsafe	• Supports dynamic operation and identifies misbehaving servers in the cloud • Greatly improves data storage security in cloud computing.
NTPA [51]	• RSA: used for encryption algorithm and Bilinear Diffie-Hellman: used to secure the keys while exchanging them Bilinear Diffie-Hellman is the proper method to exchange keys which allows two entities to share secret keys without any prior knowledge	• Data storage security	• Reduces computing complexity • Assuring confidentiality • Authentication is secured • Unauthorized access is restricted
PoOR [52]	• For guaranteeing security, this scheme uses erasure code, Merkle tree, and homomorphic verifiable tags • Efficiency analysis is conducted with the help of parameters such as data size, computation complexity, size of metadata, and communication cost	• Data duplication is a problem that increases data redundancy	• The requirement of the cloud environment is satisfied with this scheme • Optimized traffic cost • Computation performance is relatively satisfactory
OPoR [53]	• The different entities present in this scheme are the Client, • Cloud Storage Server, and Cloud Audit Server • Remotely filed stored are audited by using a cloud server that is independent of the storage server	• Reset attacks occur during the upload phase against storage	• Significantly reduced • computation overhead • Both dynamic data operation and public verifiability are supported
SCPV [54]	• Uses proof of retrievability technique for public verification • Consists of public certificateless verification, security, and efficiency	• Verification cost is higher • Multiple verification tasks are not performed	• A malicious auditor user cannot impact the security of SCLPV • Large verification overhead guarantees the security of the data
PNL [55]	• PNL mechanism is based on description logic • To guarantee the availability, erasure code in file distribution is used • Public auditing is required for stored data; hence, TPA is used	• Does not guarantee the security of user private data	• Protects the user data from being misused • Protects against Byzantine failures by dynamic data operation and server colluding attacks in the cloud
DEDP [56]	• Based on a feedback audit scheme • Utilizes a lightweight protocol, and adopts multiple TPAs for computational audits • Three phases: setup, release, and execution • The user performs the final verification task	• Processing proofs are required • Running time analysis should be performed	• Frame and colluding attacks are prevented
PASNSD [57]	• This scheme utilizes the Oruta and Knox approach, and the digital signature makes it more secure • The integrity of the shared data during the auditing process should be preserved	• A rival may corrupt the data in the verification phase and prevent user from using correct data	• Storage correctness is preserved when the cloud server fails to authenticate its response
TSAS [34]	• Utilizes the combination of cryptography and the bi-linearity property for multicloud batch auditing • The requirements of the protocol are confidential • Dynamic auditing and batch auditing	• Auditing protocol becomes insecure due to dynamic operations • Replay attack and forge attack occurs	• Data privacy is protected against the auditor and applicable to large-scale cloud storage systems • Less communication and computation costs
MTTPA [59]	• A novel security auditing framework to maintain trust by choosing the proper cloud service provider. This structure is based on a consensus assessments initiative questionnaire (CAIQ). TPA does the validation tasks • This framework helped to demonstrate the security strength designed by the Cloud Service Alliance	• A cloud service user feedback is not supported	• A security strength is demonstrated to be effective

Table 3. *Cont.*

Security Model	Security Requirements	Threats	Advantages
ESTTP [35]	• Based on the trusted third party-based scheme to encrypt the cloud data and algorithms • Encrypt the cloud data and algorithms • Uses a secret key for communication. TPA performs user authentication and ensures data integrity	• High communication overhead	• Improved data confidentiality • It is described as reducing the computational burden
CTM [61]	• Based on a centralized model approach • Uses the feedback mechanism from CSU to obtain trust values	• Cloud service user feedback cannot always be trusted	• Trust is significantly established for cloud users • Updating changes in the server is made easy
TPPCSS [62]	• Cloud data are divided into several parts using the Hash–Solomon algorithm • Cloud server, fog server, and local machine are the three main parts in this scheme • Encoding and decoding are performed to prove the effectiveness of the scheme	• Users do not have control over physical storage	• Maximum efficiency is achieved • Encoding procedures ensure the privacy of the data

6. TPA-Based Security Challenges and Recommendations

Existing countermeasures and solutions for restricting the malicious intent of the TPA are not enough. TPA acts as a verifier that should not be trusted if data privacy protection in the public cloud is the target. RSA-based storage security is utilized to recognize malicious TPA intent. Data encryption techniques can reduce computation costs and enhance data confidentiality. However, private keys are considered to be unsafe that can be compromised by TPAs. The Knox and Oruta methods are used to protect data privacy, but these methods might be corrupted by the malicious TPA while performing the verification processes. The privacy negotiation mechanisms are introduced to protect cloud entities against Byzantine failures and colluding attacks. Nevertheless, these mechanisms guarantee data protection due to the attack of TPA. The Privacy-preserving auditing models have been utilized to mitigate the malicious intent of the TPA, but these approaches inheriting the negative features of high time-complexity and additional bandwidth consumption. Third-party storage audit services methods have been used to preserve data privacy. These methods are capable to reduce the communication cost, but they affect the security of used auditing protocols. The public auditing mechanisms are proposed to reduce the communication and computation costs and protect data privacy from malicious TPA. However, an internal attack of the TPA might be a serious issue. Managing trust in TPAs could provide effective security protection. Nevertheless, this mechanism does not support cloud client feedback. High levels of cloud client trust can be achieved using a centralized trust model. This mechanism facilitates updating changes; however, feedback reported by cloud clients should not always be trusted. When the TPA applies random masking and homomorphic nonlinear techniques, a decent efficiency is achieved even if the TPA is carrying out various auditing tasks. However, the TPA can be able to obtain a local copy of the data. Data possession models can be utilized in cloud paradigms to provide decent anonymity. However, these models are not particularly designed for TPA.

Addressing the security challenges of data privacy, lightweight security privacy-preserving models could be the better option to handle the TPAÕ malicious intent. These models can provide authentication and confidentiality by using mutual authentication and secret data sharing.

Furthermore, utilizing mutual authentication can decrease the cost of information exchange. The secure certificateless public verification methods can be utilized to combat malicious TPA. Reliability can also significantly be improved by using a designated public verifier. This technique can also decrease computation complexity. The layered interleaving models can be employed during auditing to efficiently recover singleton losses. Nonetheless, data contents should not be exposed to the TPA.

Table 4 demonstrates the strengths/weaknesses of the existing solutions proposed for the malicious TPA and recommendations.

Table 4. Strengths and weaknesses of the existing solutions proposed for the malicious intent detection of the TPA and recommendations for choosing better model.

Existing Solutions against Malicious TPA	Strength	Weakness	Recommendations/Remarks
RSA-based storage security mechanisms	Reducing computational cost and enhance data confidentiality	Can be compromised by TPA	These methods are not completely suitable to determine the malicious intent of the TPA
Data encryption techniques	Enhancing data confidentiality	Can be compromised by TPA	These methods do not provide complete protection against malicious intent of the TPA
Knox and Oruta methods	Supportive in verification process	Might be corrupted by the malicious TPA	These methods are not particularly designed for malicious intent of the TPA
Privacy negotiation mechanisms	Protecting privacy preservation of the cloud entities against Byzantine failures and colluding attacks	Negotiator could be malicious TPA	These methods do not guarantee data protection due to attack of TPA
Privacy-preserving auditing models	Mitigating the malicious intent of the TPA	Inheriting negative features of high time-complexity and additional bandwidth consumption	These methods can reduce the malicious intent of the TPA in some particular scenarios but cannot completely provide the solution
Third-party storage audit services methods	Reducing the communication cost	The security auditing protocols can be affected	These methods do not provide perfect protection against the malicious TPA
Public auditing mechanisms for TPA	Reducing the communication and computation costs	An internal attack of the TPA might be a serious issue	These methods can work in particular scenarios but not permanent solution against TPA
Trust management TPA models	Effective security protection	No support for the cloud client feedback	These models show the domination of TPA. Therefore, the TPA can easily play the role of malicious TPA
Data possession models	Provide data anonymity	Not TPA-specific	These models are not properly designed for TPA
Centralized trust models	Achieving the trust of cloud clients and facilitates updating changes	feedback reported by cloud clients is not always trusted.	These models are not particularly designed for TPA
Random masking and homomorphic nonlinear techniques	Providing decent efficiency even if the TPA carries out various auditing tasks.	TPA can be able to obtain a local copy of the data	These methods are not supportive to determine the malicious intent of the TPA
Lightweight security privacy-preserving models	Providing authentication and confidentiality by using the mutual authentication and secret data sharing processes. Furthermore, information exchange cost can be decreased.	A few models are available for TPA, but those models are still not matured	These methods are suitable to detect the malicious intent of the TPA
Secure certificateless public verification methods	Key generation center possesses the complete power and is implicitly trusted. Trust can be built between TPA and either cloud service provider or client	Key generation center can be compromised. As a result, TPA has an access to the public key partially and private keys of all clients	These methods are good for protecting data privacy against malicious TPA, but there is a possibility that key generation center can be compromised by the TPA
Designated public verifier	Reliability can also significantly be improved. In addition, computational complexity can also be decreased	No state-of-the art models are available	These models can be supportive against the malicious intent of the TPA
Layered interleaving models	Recovering singleton losses efficiently during the auditing process. Furthermore, data contents cannot be exposed to the TPA	A few models are available but they are not fully matured	These models can protect the data privacy against the malicious intent of the TPA

7. Conclusions

In this survey, cloud security based on a third-party auditor (TPA) was extensively reviewed. The role of the TPA is to ensure the auditing for clients and to provide secure communication and data integrity. However, several issues appear when TPAs are utilized in cloud computing. Some of these issues are related to trust. Thus, we studied many research papers that address security in relation to TPAs.

In this work, the most recent TPA-based techniques were investigated and categorized based on the utilized security approaches and summarized based on security requirements. The first part of the review discussed vulnerabilities and presented how TPAs can be used to produce threats to data privacy. The major impacts in term of cloud security that

manifest when adopting TPAs were also discussed. However, adopting a TPA can come with a price: e.g., trust issues, security concerns, communication and computation costs, and data breaches. Moreover, approaches used to preserve privacy were classified using TPAs' dynamicity as a categorization method. Security weaknesses were also introduced and discussed. Lastly, recommendations and future work were suggested. To sum things up, academic researchers and industries could plan to propose a lightweight and highly secure method that enhances trust when adopting TPA in cloud computing.

Author Contributions: A.R. and M.B.H.F., conceptualization, writing, idea proposal, and methodology; B.A. and M.A., conceptualization, draft preparation, editing, and visualization. All authors have read and agreed to this version of the manuscript.

Funding: This work was partially supported by the Sensor Networks and Cellular System (SNCS) Research Center under Grant 1442-002.

Acknowledgments: Taif University Researchers Supporting Project number (TURSP-2020/302), Taif University, Taif, Saudi Arabia. The authors gratefully acknowledge the support of SNCS Research Center at the University of Tabuk, Saudi Arabia. In addition, the authors would like to thank the deanship of scientific research at Shaqra University for supporting this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Razaque, A.; Jararweh, Y.; Alotaibi, B.; Alotaibi, M.; Hariri, S.; Almiani, M. Energy-efficient and secure mobile fog-based cloud for the Internet of Things. *Future Gener. Comput. Syst.* **2021**, *127*, 1–13. [CrossRef]
2. Huang, H.; Sun, X.; Xiao, F.; Zhu, P.; Wang, W. Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. *J. Parallel Distrib. Comput.* **2021**, *148*, 46–57. [CrossRef]
3. Ibrahim, F.A.; Hemayed, E.E. Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review. *Comput. Secur.* **2019**, *82*, 196–226. [CrossRef]
4. Razaque, A.; Vennapusa, N.R.; Soni, N.; Janapati, G.S. Task scheduling in cloud computing. In Proceedings of the Systems, Applications and Technology Conference (LISAT) 2016 IEEE Long Island, Farmingdale, NY, USA, 29 April 2016; pp. 1–5.
5. Arwa, M.; Hamdan, M.; Khan, S.; Abdelaziz, A.; Babiker, S.F.; Imran, M.; Marsono, M.N. Software-defined networks for resource allocation in cloud computing: A survey. *Comput. Netw.* **2021**, *195*, 108151.
6. Yeh, T.; Chen, Y. Improving the hybrid cloud performance through disk activity-aware data access. *Simul. Model. Pract. Theory* **2021**, *109*, 102296. [CrossRef]
7. Razaque, A.; Li, Y.; Liu, Q.; Khan, M.J.; Doulat, A.; Almiani, M.; Alflahat, A. Enhanced Risk Minimization Framework for Cloud Computing Environment. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–7.
8. Kalluri, R.K.; Guru, C.V. An effective analytics of third party auditing and Trust architectures for integrity in cloud environment. *Mater. Today Proc.* **2021**, *79*, 69–76. [CrossRef]
9. Jansen, W.A. Cloud hooks: Security and privacy issues in cloud computing. In Proceedings of the IEEE 2011 44th Hawaii International Conference on System Sciences, Washington, DC, USA, 4–7 January 2011; pp. 1–10.
10. Jhawar, R.; Piuri, V. Fault tolerance and resilience in cloud computing environments. In *Computer and Information Security Handbook*, 3rd ed.; ScienceDirect: Amsterdam, The Netherlands, 2017; pp. 165–181.
11. Patel, A.; Taghavi, M.; Bakhtiyari, K.; Júnior, J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *J. Netw. Comput. Appl.* **2013**, *36*, 25–41. [CrossRef]
12. Raghav, I.; Chhikara, S.; Hasteer, N. Intrusion detection and prevention in cloud environment: A systematic review. *Int. J. Comput. Appl.* **2013**, *68*, 7–11. [CrossRef]
13. Modi, C.N.; Acha, K. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. *J. Supercomput.* **2017**, *73*, 1192–1234. [CrossRef]
14. Shamshirband, S.; Fathi, M.; Chronopoulos, A.T.; Montieri, A.; Palumbo, F.; Pescapè, A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *J. Inf. Secur. Appl.* **2020**, *55*, 102582. [CrossRef]
15. Kene, S.G.; Theng, D.P. A review on intrusion detection techniques for cloud computing and security challenges. In Proceedings of the IEEE 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 26–27 February 2015; pp. 227–232
16. Paxton, N.C. Cloud security: A review of current issues and proposed solutions. In Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), Pittsburgh, PA, USA, 1–3 November 2016; pp. 452–455.
17. Manral, B.; Somani, G.; Choo, K.K.R.; Conti, M.; Gaur, M.S. A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–38. [CrossRef]

18. Ru, J.; Yang, Y.; Grundy, J.; Keung, J.; Hao, L. A systematic review of scheduling approaches on multi-tenancy cloud platforms. *Inf. Softw. Technol.* **2020**, *132*, 106478.
19. Albugmi, A.; Alassafi, M.O.; Walters, R.; Wills, G. Data security in cloud computing. In Proceedings of the 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), London, UK, 17–19 August 2016; pp. 55–59. [CrossRef]
20. Shakarami, A.; Ghobaei-Arani, M.; Shahidinejad, A.; Masdari, M.; Shakarami, H. Data replication schemes in cloud computing: A survey. *Clust. Comput.* **2021**, *24*, 2545–2579. [CrossRef]
21. Domingo-Ferrer, J.; Farras, O.; Ribes-Gonlez, J.; Sánchez, D. Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Comput. Commun.* **2019**, *140*, 38–60. [CrossRef]
22. Karthiban, K.; Smys, S. Privacy preserving approaches in cloud computing. In Proceedings of the IEEE 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 462–467.
23. Perez-Botero, D.; Szefer, J.; Lee, R.B. Characterizing hypervisor vulnerabilities in cloud computing servers. In Proceedings of the ACM 2013 International Workshop on Security in Cloud Computing, Dresden, Germany, 9–12 December 2013; pp. 3–10.
24. Razaque, A.; Amsaad, F.; Hariri, S.; Almasri, M.; Rizvi, S.S.; Frej, M.B.H. Enhanced grey risk assessment model for support of cloud service provider. *IEEE Access* **2020**, *8*, 80812–80826. [CrossRef]
25. Razaque, A.; Nadimpalli, S.S.V.; Vommina, S.; Atukuri, D.K.; Reddy, D.N.; Anne, P.; Vegi, D.; Malllapu, V.S. Secure data sharing in multi-clouds. In Proceedings of the IEEE 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 1909–1913.
26. Dunne, N.J.; Brennan, N.M.; Kirwan, C.E. Impression management and Big Four auditors: Scrutiny at a public inquiry. *Account. Organ. Soc.* **2021**, *88*, 101170. [CrossRef]
27. Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y.; Vasilakos, A.V. Security and privacy for storage and computation in cloud computing. *Inf. Sci.* **2014**, *258*, 371–386. [CrossRef]
28. Hussien, Z.A.; Jin, H.; Abduljabbar, Z.A.; Yassin, A.A.; Hussain, M.A.; Abbdal, S.H.; Zou, D. Public auditing for secure data storage in cloud through a third-party auditor using modern ciphertext. In Proceedings of the IEEE 2015 11th International Conference on Information Assurance and Security (IAS), Marrakech, Morocco, 14–16 December 2015.
29. Wang, B.; Li, B.; Li, H. Panda: Public auditing for shared data with efficient user revocation in the cloud. *IEEE Trans. Serv. Comput.* **2013**, *8*, 92–106. [CrossRef]
30. Pavithra, S.; Thangadurai, E.; Mailsamy, M. Secure Data Storage in Cloud using Code Regeneration and public audition. *Int. J. Emerg. Technol. Comput. Sci. Electron.* **2016**, *20*, 65–68.
31. Razaque, A.; Rizvi, S.S. Privacy preserving model: A new scheme for auditing cloud stakeholders. *J. Cloud Comput.* **2017**, *6*, 7. [CrossRef]
32. Shrinivas, D. Privacy-preserving public auditing in cloud storage security. *Int. J. Comput. Sci. Nad Inf. Technol.* **2011**, *2*, 2691–2693.
33. Shen, W.; Yu, J.; Xia, H.; Zhang, H.; Lu, X.; Hao, R. Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third-party medium. *J. Netw. Comput. Appl.* **2017**, *82*, 56–64. [CrossRef]
34. Wang, B.; Li, B.; Li, H. Knox: Privacy-preserving auditing for shared data with large groups in the cloud. In Proceedings of the International Conference on Applied Cryptography and Network Security, Kamakura, Japan, 21–24 June 2012; Springer: Berlin/Heidelberg, Germany, 2012.
35. Girma, A.; Garuba, M.; Li, J. Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics. In Proceedings of the 2015 12th International Conference on Information Technology-New Generations, Las Vegas, NV, USA, 13–15 April 2015; pp. 206–211.
36. Anbuchelian, S.; Sowmya, C.M.; Ramesh, C. Efficient and secure auditing scheme for privacy preserving data storage in cloud. *Clust. Comput.* **2019**, *22*, 9767–9775. [CrossRef]
37. Worku, S.G.; Xu, C.; Zhao, J.; He, X. Secure and efficient privacy-preserving public auditing scheme for cloud storage. *Comput. Electr. Eng.* **2014**, *40*, 1703–1713. [CrossRef]
38. Gajendra, B.P.; Singh, V.K.; Sujeet, M. Achieving cloud security using third party auditor, MD5 and identity-based encryption. In Proceedings of the IEEE 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 1304–1309.
39. Yang, K.; Jia, X. An efficient and secure dynamic auditing protocol for data storage in cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *24*, 1717–1726. [CrossRef]
40. Moghaddam, F.F.; Karimi, O.; Alrashdan, M.T. A comparative study of applying real-time encryption in cloud computing environments. In Proceedings of the 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, CA, USA, 11–13 November 2013; pp. 185–189.
41. Kundu, N.; Debnath, S.K.; Mishra, D. A secure and efficient group signature scheme based on multivariate public key cryptography. *J. Inf. Secur. Appl.* **2021**, *85*, 102776.
42. Wang, B.; Li, H.; Li, M. Privacy-preserving public auditing for shared cloud data supporting group dynamics. In Proceedings of the 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 9–13 June 2013.
43. Wang, Q.; Wang, C.; Ren, K.; Lou, W.; Li, J. Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 847–859. [CrossRef]

44. Wu, T.Y.; Lin, Y.; Wang, K.H.; Chen, C.M.; Pan, J.S.; Wu, M.E. Comments on a privacy preserving public auditing mechanism for shared cloud data. In Proceedings of the ACM 4th Multidisciplinary International Social Networks Conference on ZZZ, Bangkok, Thailand, 17–19 July 2017.
45. Rizvi, S.; Razaque, A.; Cover, K. Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment. In Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 3–5 November 2015.
46. Rizvi, S.; Razaque, A.; Cover, K. Cloud Data Integrity Using a Designated Public Verifier. In Proceedings of the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, New York, NY, USA, 24–26 August 2015.
47. Ren, Y.; Yang, Z.; Wang, J.; Fang, L. Attributed Based Provable Data Possession in Public Cloud Storage. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, 27–29 August 2014.
48. Hao, Z.; Yu, N. A multiple-replica remote data possession checking protocol with public verifiability. In Proceedings of the 2010 Second International Symposium on Data, Privacy, and E-Commerce, Buffalo, NY, USA, 13–14 September 2010.
49. Erway, C.C.; Küpçü, A.; Papamanthou, C.; Tamassia, R. Dynamic provable data possession. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2015**, *17*, 15. [CrossRef]
50. Wang, C.; Wang, Q.; Ren, K.; Lou, W. Privacy-preserving public auditing for data storage security in cloud computing. In Proceedings of the 2010 Proceedings IEEE Infocom, San Diego, CA, USA, 14–19 March 2010.
51. Jianhong, Z.; Hua, C. Secuirty storage in the cloud computing: A rsa-based assumption data integrity check without original data. In Proceedings of the 2010 International Conference on Educational and Information Technology, Chongqing, China, 17–19 September 2010.
52. Yang, C.N.; Lai, J.B. Protecting data privacy and security for cloud computing based on secret sharing. In Proceedings of the 2013 International Symposium on Biometrics and Security Technologies, Chengdu, China, 2–5 July 2013.
53. Zheng, Q.; Xu, S. Secure and efficient proof of storage with deduplication. In Proceedings of the Second ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 7–9 February 2012.
54. Zheng, Q.; Xu, S. Fair and dynamic proofs of retrievability. In Proceedings of the First ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 21–23 February 2011.
55. Singh, R.; Kumar, S.; Agrahari, S.K. Ensuring Data Storage Security in Cloud Computing. *IOSR J. Eng.* **2012**, *2*, 12. [CrossRef]
56. Zhang, Y.; Pan, J.; Qi, L.; He, Q. Privacy-preserving quality prediction for edge-based IoT services. *Future Gener. Comput. Syst.* **2021**, *114*, 336–348. [CrossRef]
57. Huang, L.; Zhang, G.; Fu, A. Privacy-preserving public auditing for non-manager group. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
58. Yang, K.; Jia, X. TSAS: Third-Party Storage Auditing Service. In *Security for Cloud Storage Systems*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 7–37.
59. Zhu, Y.; Wang, H.; Hu, Z.; Ahn, G.J.; Hu, H.; Yau, S.S. Dynamic audit services for integrity verification of outsourced storages in clouds. In Proceedings of the 2011 ACM Symposium on Applied Computing, TaiChung, Taiwan, 21–24 March 2011.
60. Sharma, N.; Tyagi, S.; Atri, S. A Survey on Heuristic Approach for Task Scheduling in Cloud Computing. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 3.
61. Shimbre, N.; Deshpande, P. Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. In Proceedings of the IEEE 2015 International Conference on Computing Communication Control and Automation, Pune, India, 26–27 February 2015.
62. Kaur, M.; Mahajan, M. Using encryption algorithms to enhance the data security in cloud computing. *Int. J. Commun. Comput. Technol.* **2013**, *1*, 56–59.
63. Suresh, K.; Prasad, K. Security issues and Security algorithms in Cloud Computing. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2012**, *2*, 110–114.
64. Akbari, E.; Cung, F.; Patel, H.; Razaque, A.; Dalal, H.N. Incorporation of weighted linear prediction technique and M/M/1 Queuing Theory for improving energy efficiency of Cloud computing datacenters. In Proceedings of the 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 29 April 2016; pp. 1–5.