




Article

Privacy preservation Models for Third-Party Auditor over Cloud Computing: a Survey

Abdul Razaque¹ , Mohamed Ben Haj Frej², Bandar Alotaibi^{3,4*} , Munif Alotaibi^{5*} 

¹ Department of Computer Engineering and Information Security, International Information Technology University, Kazakhstan; a.razaque@iitu.kz

² Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT, USA; mbenhaj@bridgeport.edu

³ Department of Information Technology, University of Tabuk, Tabuk 47731, Saudi Arabia; b-alotaibi@ut.edu.sa

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; munif@su.edu.sa

* Correspondence: b-alotaibi@ut.edu.sa, munif@su.edu.sa

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-art of cloud computing's privacy-preserving models (PPM) based on a TPA. Three TPA factors of paramount significance have been discussed: TPA involvement, security requirements, and security threats caused by vulnerabilities. Moreover, TPA's privacy preserving models have been 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 Client (CC); Cloud computing; Cloud Service Provider (CSP); Security; Service Level Agreement (SLA); Privacy-Preserving Model (PPM); Third-party auditor (TPA)

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 [1–6]. 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' point of views, and are presented as IT-related skills, reachable with no in-depth familiarity of the used technologies, and with a titular coordinating effort.

The cloud as a concept can be defined as "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 [7]. Four diverse types of delivery models are supported in cloud computing: private cloud, public cloud, hybrid cloud, and community cloud [8–12].

- 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 and 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-premise 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 the security and lowers the price. However, the high management complexity is the major drawback [13].
- 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 and ambiguities still exist which make many organizations reluctant to fully utilize cloud computing [14].

In cloud computing, data security, privacy, and safety are fundamental measurements 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 at their convenient. 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 [15,16].

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 [17–20]. To deal with privacy and security challenges, TPA terminology is presented. Cloud clients and cloud providers lack some capabilities which make the TPA (i.e. that has these capabilities) an essential entity in the cloud realm. The TPA can be trusted from both cloud clients and cloud providers to evaluate the security level of cloud service providers' storage, thus, the data can be marked as protected against malicious attempts, Byzantine failures, data alteration attacks, and even server colluding attacks [21–24]. 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 operation (depicted in Figure 1).

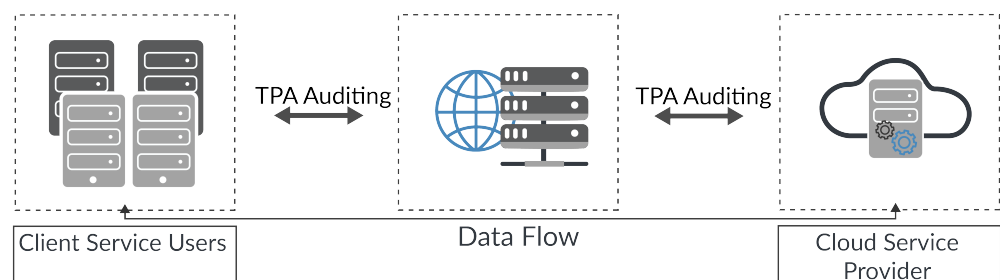


Figure 1. Auditing process based on a TPA.

The cloud security deficiencies are the major factor 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:

- We comprehensively discuss the state-of-the-art, in research, privacy-preserving TPA-based models designated for cloud computing.
- We extensively discuss the security shortcomings that open a backdoor for malicious TPAs that might misuse the service and create data privacy threats.
- Focusing only on dynamicity, privacy-preserving models for cloud computing based on a TPA are classified and categorized.
- The scientific research questions about privacy-preserving models are raised.
- We present each privacy-preserving model limitations and provide some recommendations for future work.

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 the security elements, vulnerabilities, and potential threats. We summarize and recapitulate all the studied methods in Section 5. Section 6 discusses the TPA-based security solutions and recommendation. And 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 to block the malicious role of the TPA? What are the security requirements to maintain 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 of 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 are supportive for collecting the articles to discuss the state-of-art of cloud computing's privacy-preserving models. Different keywords have been used to locate the articles, such as categorization of PPM based on a TPA. The involvement of a TPA for exploiting the data privacy including the security requirements as well as the vulnerabilities that lead to security threats from the TPA. The search returned numerous articles, but 116 articles have carefully been chosen that highly relate to our review, as shown in Figure 2. Twenty-four articles have been used to write the introduction section, 12 are related to the existing reviews/surveys on the security of cloud computing, 24 articles are related to the security requirements, vulnerabilities, and threats, and 51 articles are 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 elements of security requirements.



Figure 2. Number of previously published articles as organized in this review.

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, [25] presented a systematic review on Intrusion Detection and Prevention Systems (IDPS) and alarm management techniques.

The authors of [26] put forward a comprehensive taxonomy on Intrusion Detection and Prevention Systems for Cloud Computing. In [27], 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 [28], 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 [29] present 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 multi-tenancy, is an option to reduce the cost of hosting. In [30], the authors put forward a review on the current issues that could emerge from multi-tenancy and then, proposed solutions to mitigate them. In [31], the authors presented a survey on the impact of multi-tenancy when it comes to cloud forensics challenges and solutions. In [32], the authors suggested a systematic review of scheduling approaches on multi-tenancy scheduling approaches in cloud platforms. In [33], the authors presented a loophole in data security in cloud computing when we run a guest OS over a hypervisor without knowing the reliability of the guest OS. The authors of [34] 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 [35] surveyed the methods, products, challenges, and reviewed masking practices for outsourced data based on data splitting and anonymization, in addition to cryptographic techniques covered in other surveys. In [36], 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 have discussed different aspects of security in cloud computing.

4. Security elements, vulnerabilities, and potential threats

4.1. Security elements

The security requirements that play a significant role in the computing environment consist of the following elements (depicted in Figure 3):

- Confidentiality
- Integrity
- Availability
- Access Control
- Authentication

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

Existing reviews/Survey	Summary	Scope and Focus
[25], [26], [27], [28], and [29]	Review of Intrusion Detection and Prevention Systems (IDPS) in Cloud Computing	These papers cover the Intrusion Detection and Prevention Systems (IDPS)
[30], [31], and [32].	Review the cloud vulnerabilities from the multi-tenancy perspective	The authors mainly cover multi-tenancy threats
[33] and [34]	Comprehensive reviews are conducted on the data security from the cloud computing perspective.	The authors cover data security
[35] and [36]	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

- Authorization
- Accountability
- Privacy
- Non-repudiation

4.1.1. Confidentiality

Confidentiality refers to limiting the access to the protected data to exclusively the authorized parties. In cloud computing, threats of data breaches are significantly higher than on-promise information technology. The increase in the number of access points is related to the growing number of involved parties, devices, and applications. In cloud computing, data confidentiality is linked to client authentication. Protecting clients' accounts from theft is an example of a larger issue related to restricting access to entities, such as memory, hardware, and software.

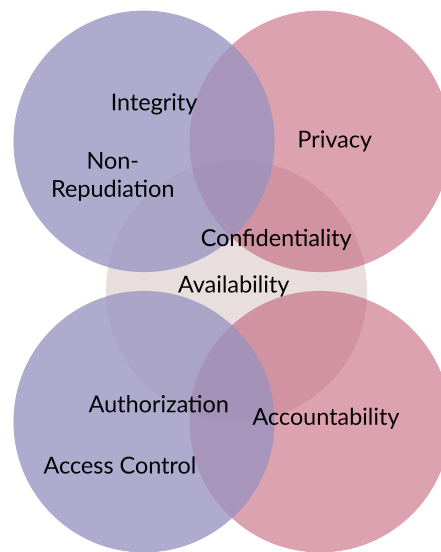


Figure 3. Cloud computing's elements of security requirements.

4.1.2. Integrity

Integrity emphasizes that assets (either software assets or hardware assets) associated with data would only be altered by authorized entities and within the authorized procedures. Data integrity [37] is defined as a mechanism that preserves data in transit from unauthorized modification, fabrication, or deletion [38].

4.1.3. Availability

Availability guarantees the system is accessible and can be used by authorized parties upon demand. The continuity of operations even with the existence of the misuse can be referred to as system availability. The system must normally operate even if there is a security breach.

4.1.4. Access control

In a multi-tenancy setting, access control breaches could be caused by interoperability deficiencies; in which identification and authentication requirements are affected. Similar to availability, the retrieval of data is complicated if the data or a specific service is not available on demand. The security breaches could be increased if different mechanisms are used by heterogeneous cloud servers (i.e., this is known as policy integration). Due to the increasing number of tenancies, data on public clouds might be threatened by attackers and data brokers. One possible type of attack is eavesdropping, using a software like Easter eggs [40].

4.1.5. Authentication

Authentication provides a way of detecting a client, typically by having the client enter a valid client name and correct password before getting approved to access the resources on the cloud servers. The process of authentication depends on each client, and involves a specific set of standards for obtaining access. If the credentials of the client are matched, then the client is granted access to the cloud servers. If the credentials do not match, then the access is blocked [41,42].

4.1.6. Authorization

This process defines whether the client possesses the authority to release commands. The authorization process is enforced. It also determines what types of resources, activities, or services a client is granted as the authorization happens within the perspective of

authentication. Once the client is authenticated, then they may be authorized for several types of activities [43,44].

4.1.7. Accountability

This provides the tracking of the user activities and the record-keeping on a cloud server for a given period. The accountability includes real-time services [58] on accessing the cloud servers, the cloud services obtained or employed, trend analysis, capacity, cloud cost allocations, login data for client authentication and authorization, billing data, and the data. A TPA supported by trusted services and tools can provide shareholders with suitable views of stored data and how it is handled and safeguarded.

4.1.8. Privacy

Restrictions on private data from illegitimate clients' access are referred to as privacy. Privacy issues are gaining significance in the online world. Privacy promotes the client's confidence and economic progress [47,48]. However, the secure management, control, and release of personal and private information into the cloud servers signify massive challenges for all shareholders, involving burdens from both commercial and legal perspectives.

4.1.9. Non-repudiation

This is the way to assure that users do not disown some of their activities [49]. Non-repudiation is an authorized notion that is widely used in cloud computing and refers to a service that offers proof of data origin and data integrity. Digital signatures, as well as other security measures, provide non-repudiation when making online transactions.

4.2. 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 5) that might mutate cloud clients' hopes of increasing scalability and decreasing coordination cost into a misery of misuse and data breaches [50]. Therefore, the security issues associated with cloud adoption should be considered [51]. The most common vulnerabilities effecting TPAs are given as follows:

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

4.2.1. 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 [52]. 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 [53].

Let us consider the server S_c in the CSP and clients $C = \{C_1, C_2, \dots, C_k\}$ that use the services $S = \{S_1, S_2, \dots, S_k\}$. We take the security requirements $R_{se} = \{R_{se1}, R_{se2}, \dots, R_{se-n}\}$ to impose on the server. Thus, the risk $R_{p,q}$ can be referred to as $R_{p,q}$, for $1 \leq p \leq k$ & $1 \leq q \leq n$ 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:

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

4.2.2. 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 [54]. 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 [55,56]. If CSP is reliably providing the services, then there is the possibility that 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 authors of [57] introduced a trust model based on the time factor. In the proposed model, a 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:

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

Where ω is used for the faster time decay, δ is feedback received from the clients, t is 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 a responsibility to evaluate and authenticate the client while maintaining privacy preservation depicted in Figure 4. This is carried out as actions taken by the TPA could be malicious for the client and CSP [58].

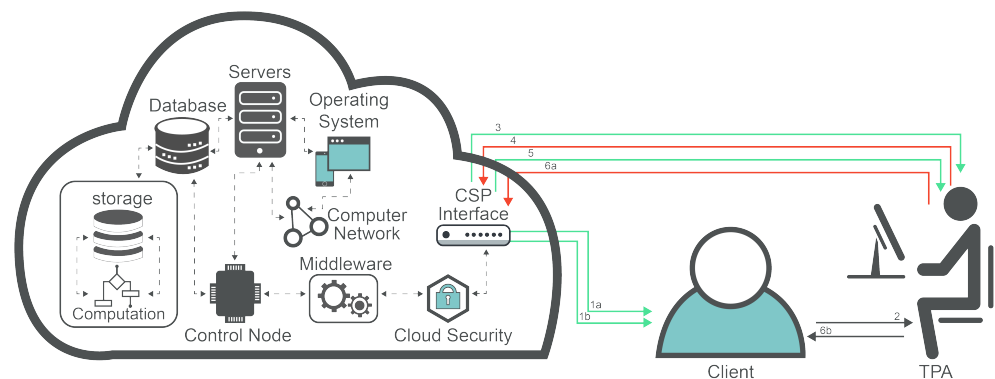


Figure 4. Evaluation and authentication of the client through CPS.

The cloud clients should be aware of the following seven issues [59].

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

4.3. TPA-based cloud threats

Several security requirements are violated because of the diverse attacks that target cloud computing as depicted in Figure 5.

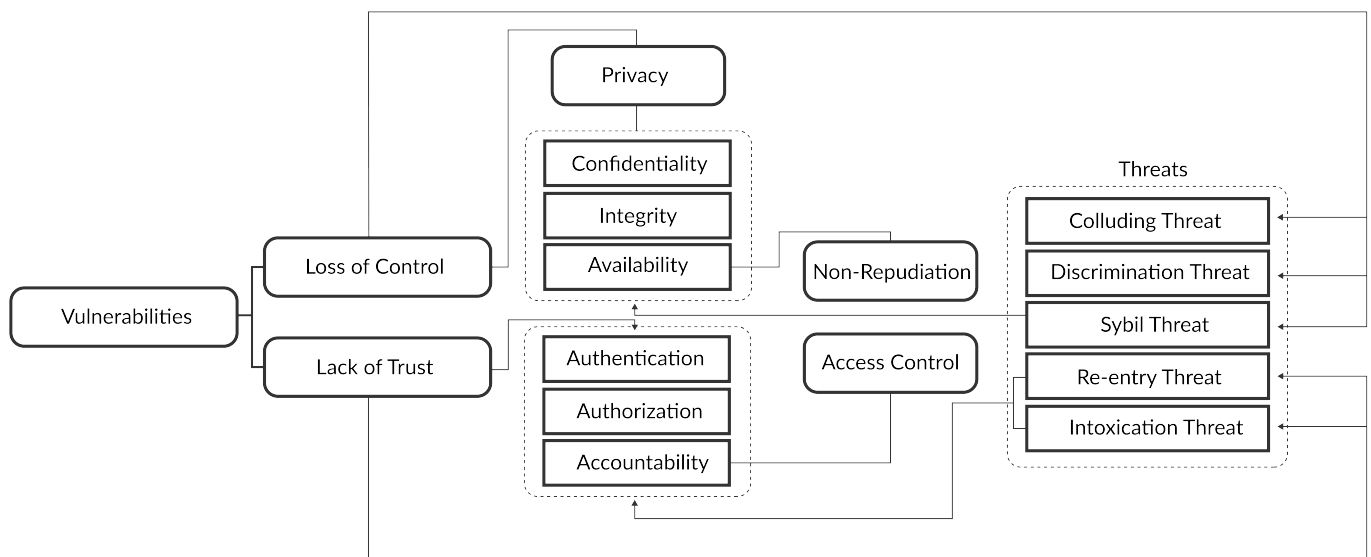


Figure 5. Security requirements, vulnerabilities, and threats.

4.3.1. 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 [61]. 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.

4.3.2. Sybil threats

This type of attack is launched by malicious cloud clients utilizing several identities to tamper with test outcomes [61]. 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. Noor et al. [60] detect both Sybil and collusion attacks using a credibility approach.

4.3.3. ON OFF threat or intoxication threat

Malicious cloud clients adjust their behaviors either to act as harmful or harmless users [62]. 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 [62]. This attack can be resolved using a forgetting factor approach.

4.3.4. 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 [62]. Mitigating or preventing this attack is a difficult task to accomplish.

4.3.5. 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 [62]. 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 are paramount for protecting the privacy of the data and information.

5.1.1. Security and privacy for storage

Wei et al. [63] 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 caution when they share their sensitive information with with a coexisting TPA. The authors proposed the following five algorithms to encrypt the data using RSA and then apply the auditing mechanism:

- "KeyGen": this algorithm is utilized by the cloud client to generate the public key encryption pair (i.e., the public key and the private key);
- "Outsource": this algorithm is also employed by the cloud client to transfer the data to the CSP;
- "Audit": this algorithm is utilized by the TPA to transmit the audited query to the CSP;
- "Prove": 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;
- "Verify": 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 has been 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.

5.1.2. PANDA public auditing (PPA)

Cong et al. [65] 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 encryption to enable secure communication between cloud clients and TPAs. This approach provides two services: storage and data integrity.

Table 2. Recapitulation based on the key schemes [120].

Method	KEY-GEN	SIG-GEN	GEN-PROOF	Verify-PROOF	Homomorphic Linear Authenticator	Bilinear Signature	Symmetric Key	Data Security	Generating Signature
SPS [63]	✓		✓	✓					
PPA [64]	✓	✓	✓	✓					
PPPAS [65]	✓	✓	✓	✓	✓				
SEPPPA [67]	✓	✓	✓	✓					
DPVPPM [77]								✓	
EPASS [82]	✓	✓			✓	✓			
RSASS [84]									✓
TSAS [109]						✓			
ESTTP [112]							✓		

In this approach, the outsourced data does 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 side, the TPA utilizes the "KeyGen" algorithm to generate the challenge key, and the "SigGen" algorithm to verify the key. Then, the processed data is encrypted by the TPA to create the crypto-metadata; this metadata is 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. [64] 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 of [65] 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. [66]. 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 the entire data) has been presented by Pavithra et al. [67]. This approach utilizes batches for auditing and for preserving privacy and integrity. The authors utilized the bilinear map for data encryption [68]. The proposed protocol employs four algorithms: "KeyGen", "SigGen", "ProofGen", and "VerifyProof". 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. The second, private key is generated for the cloud client. The "SigGen" algorithm is utilized to generate signatures for the outsourced files. The "ProofGen" algorithm is employed by the CSP to generate integrity proof after receiving the challenge. The "VerifyProof" algorithm is used by the TPA to verify data integrity by utilizing the public key of the CSP [69]. 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 [70]. It is known that both the retrieval and outsourcing overhead is unavoidable; therefore, the authors concentrated on the challenge-response overhead. Thus, it has been deduced that the complexity of the system is constant [71].

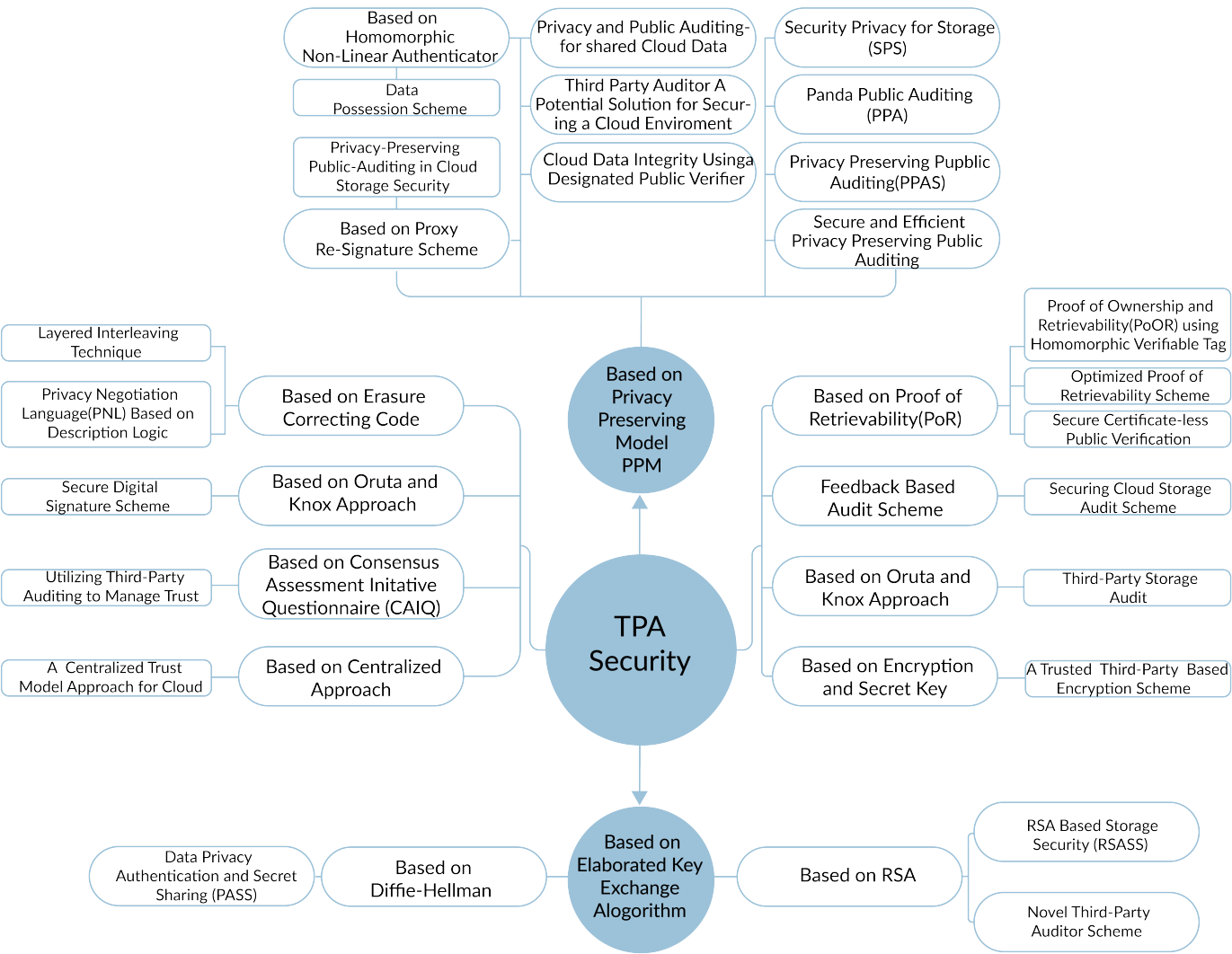


Figure 6. TPA Classification based on the Security Methods.

5.1.5. Privacy-preserving public auditing for shared cloud data

Kundu et al. [72] 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 the whole 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 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 the entire 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 low error detection rate. The major characteristic of this approach is its high-dynamic group efficiency.

Wang et al. [73] 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 multi-client 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 [74] discusses the possibility of forgery attacks and data corruption attacks, and in a follow-up work Wu et al. [75] discuss 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. [75] 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 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 work from Wu et al. [75] discusses 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 is developed to audit the stakeholders in the cloud. An experiment is performed to show a malicious insider in TPA and the authentication process in the cloud service provider. The main parameters observed are effectiveness, operational efficiency, successful rate and reliability of CSP. This method protects the user's outsourced data in the cloud [76].

5.1.9. Cloud data integrity using a designated public verifier

A public verifier is presented by Razaque et al. [77] 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 non-linear authenticator

The authors of [78] 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 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. 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 is still at risk if the TPA is not trustworthy [79,80].

5.1.11. Based on the proxy re-signature scheme

Erway et al. [81] presented a technique to protect cloud storage and conceal users' data from the TPA. This approach relies on random masking and a homomorphic non-linear authenticator to prevent TPAs from learning any users' data while auditing. Non-linear 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. [82] 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 pre-computation 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. [83]. 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 done 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 [84]: 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, misbehaving servers are identified and 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 [85].

5.2.2. Novel third party auditor scheme

This method consists of two phases [86]; 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 have occurred in the cloud server, the cloud server must inform the organization's server.

5.3. Based on Diffie-Hellman

5.3.1. 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 [87,88].

- 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 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 multi-serve 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 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 security analysis and proves its robustness against obtaining the key, even if the client's device is compromised [89].

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 proof of retrieving information in environments in which both the server and client are not fully trustworthy. Yan et al. [90] proposed an approach to address this issue, which was based on proofs of ownership and retrievability (PoOR) [91]. 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 [92,93].

5.4.2. optimized proof of retrievability scheme

Zheng et al. [94] proposed an approach using two independent 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 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 full protection against reset attacks. The reset attack can be triggered at the upload stage by the cloud storage [95,96].

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 [97] 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) which 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 [98].

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 pre-computes 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 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 [101,102]. 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 [103].

Table 3. TPA classification by requirements [120].

Security Model	Security Requirements	Threats	Advantages
SPS [63]	<ul style="list-style-type: none"> • Third party auditing • Supports data dynamics • Supports privacy-preserving public auditing • Use of private channels to relay information 	<ul style="list-style-type: none"> • TPA somehow trusted • Cost not low enough 	<ul style="list-style-type: none"> • Cost efficient • Practical for cloud systems on large-scales • Considers vulnerabilities of dynamic data • Communication overhead
PPA [68]	<ul style="list-style-type: none"> • Third party auditing • Supports data dynamics • Double block transportation • Supports privacy-preserving public auditing 	<ul style="list-style-type: none"> • TPA used as an intermediary to send encrypted data • Hidden server failure 	<ul style="list-style-type: none"> • Cost efficient • Practical for cloud systems on a large scale • TPA does not need a local copy of data
PPPAS [70]	<ul style="list-style-type: none"> • Third party auditing • Supports batch auditing • Supports privacy-preserving public auditing 	<ul style="list-style-type: none"> • Relies on TPA 	<ul style="list-style-type: none"> • TPA does not need a local copy of data • Identification of Invalid Response • Support for Dynamic Data
SEPPPA [71]	<ul style="list-style-type: none"> • Third party auditing • Supports batch auditing • Supports privacy-preserving public auditing 	<ul style="list-style-type: none"> • TPA somehow trusted 	<ul style="list-style-type: none"> • TPA does not need a local copy of data • Pioneer in privacy-preserving schemes for cloud
PPPASCD [72]	<ul style="list-style-type: none"> • 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 done by dynamic broadcast; to distribute the private key to the active group members securely 	<ul style="list-style-type: none"> • TPA consumes more time and bandwidth to achieve high error detection probability 	<ul style="list-style-type: none"> • Highly efficient for dynamic groups • Public auditability and data are dynamic for a remote data integrity check
MPPA [74]	<ul style="list-style-type: none"> • possibility of a forgery attack and data corruption attack • Setup phase, signing phase, proof generation, and verification 	<ul style="list-style-type: none"> • False verification is possible 	<ul style="list-style-type: none"> • Adversary attacks are minimized compared to the original scheme
SCETPA [75]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • The public verifier is not trusted 	<ul style="list-style-type: none"> • Malicious insiders and threats are reduced • Data privacy is protected
PPMACS [76]	<ul style="list-style-type: none"> • Analyze the various vulnerabilities in data stored in the cloud by securing the TPA • Effectiveness, operational efficiency and reliability are measured 	<ul style="list-style-type: none"> • The malicious insider in TPA 	<ul style="list-style-type: none"> • The effective authentication process for auditing stakeholders
DPVPPM [77]	<ul style="list-style-type: none"> • 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 like TPA 	<ul style="list-style-type: none"> • Multiple auditing is not supported 	<ul style="list-style-type: none"> • Efficiency and reliability are much improved • Computational burden is reduced
DPS [78]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Cloud storage server cannot be trusted • TPA should be trustworthy 	<ul style="list-style-type: none"> • Maintains strong anonymity in the cloud environment • Good resistance
PPACSS [81]	<ul style="list-style-type: none"> • Uses homomorphic non-linear 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 	<ul style="list-style-type: none"> • A local copy of the data can be presented in the TPA 	<ul style="list-style-type: none"> • User's outsourced data is secured in the cloud • TPA achieves better efficiency while performing multiple auditing tasks
RSASS [84]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • TPA has the private key which could be unsafe 	<ul style="list-style-type: none"> • Supports dynamic operation and identifies misbehaving servers in the cloud • Greatly improves data storage security in cloud computing.
NTPA [86]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Data storage security 	<ul style="list-style-type: none"> • Reduces computing complexity • Assuring confidentiality • Authentication is secured • Unauthorized access is restricted
PoOR [90]	<ul style="list-style-type: none"> • For guaranteeing security, this scheme uses erasure code, Merkle tree, and homomorphic verifiable tags • Efficiency analysis is done with the help of parameters like data size, computation complexity, size of metadata, and communication cost 	<ul style="list-style-type: none"> • Data duplication is a problem that increases data redundancy 	<ul style="list-style-type: none"> • The requirement of the cloud environment is satisfied with this scheme • Optimized traffic cost • Computation performance is relatively satisfactory
OPoR [94]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Reset attacks occur during the upload phase against storage 	<ul style="list-style-type: none"> • Significantly reduced computation overhead • Both dynamic data operation and public verifiability are supported
SCPV [97]	<ul style="list-style-type: none"> • Uses proof of retrievability technique for public verification • Consists of public certificate-less verification, security, and efficiency 	<ul style="list-style-type: none"> • Verification cost is higher • Multiple verification tasks are not performed 	<ul style="list-style-type: none"> • A malicious auditor user cannot impact the security of SCLPV • Large verification overhead guarantees the security of the data
LIT [99]	<ul style="list-style-type: none"> • Erasure-correcting code to tolerate multiple failures • TPA delegates the task of verification to save time on the user's side • Based on token challenge verification, correctness verification 	<ul style="list-style-type: none"> • During data auditing, the TPA does not have access to the user's data content 	<ul style="list-style-type: none"> • Highly efficient in recovering the singleton losses • Recovering the bursty data losses
PNL [101]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Does not guarantee the security of user private data 	<ul style="list-style-type: none"> • Protects the user data from being misused • Protects against Byzantine failures by dynamic data operation and server colluding attacks in the cloud
DEDP [104]	<ul style="list-style-type: none"> • Based on a feedback audit scheme • Utilizes a light-weight protocol, and adopts multiple TPAs for computational audits • Three phases: setup, release and execution • The user performs the final verification task 	<ul style="list-style-type: none"> • Processing proofs are required • Running time analysis should be done 	<ul style="list-style-type: none"> • Frame and colluding attacks are prevented
PASNSD [107]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • A rival may corrupt the data in the verification phase and prevent user from using correct data 	<ul style="list-style-type: none"> • Storage correctness is preserved when the cloud server fails to authenticate its response
TSAS [109]	<ul style="list-style-type: none"> • Utilizes the combination of cryptography and the bi-linearity property for multi-cloud batch auditing • The requirements of the protocol are confidential • Dynamic auditing and batch auditing 	<ul style="list-style-type: none"> • Auditing protocol becomes insecure due to dynamic operations • Replay attack and forge attack occurs 	<ul style="list-style-type: none"> • Data privacy is protected against the auditor and applicable to large-scale cloud storage systems • Less communication and computation costs
MTTPA [111]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • A cloud service user feedback is not supported 	<ul style="list-style-type: none"> • A security strength is demonstrated to be effective
ESTTP [112]	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • High communication overhead 	<ul style="list-style-type: none"> • Improved data confidentiality • It is described as reducing the computational burden
CTM [114]	<ul style="list-style-type: none"> • Based on a centralized model approach • Uses the feedback mechanism from CSU to obtain trust values 	<ul style="list-style-type: none"> • Cloud service user feedback cannot always be trusted 	<ul style="list-style-type: none"> • Trust is significantly established for cloud users • Updating changes in the server is made easy
TPPCSS [116]	<ul style="list-style-type: none"> • Cloud data is 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 done to prove the effectiveness of the scheme 	<ul style="list-style-type: none"> • Users do not have control over physical storage 	<ul style="list-style-type: none"> • Maximum efficiency is achieved • Encoding procedures ensure the privacy of the data

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

5.6.1. 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 semi-trusted, 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. [104] introduced a distributed edge differential privacy (DEDP) technique to help clients to check integrity of stored data themselves instead of relying on TPAs' services [105]. 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 is continuously transmitted by the TPA to the sever. 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 [106].

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 non-manager shared data known as Oruta and Knox. These shortcomings were discussed in [107,108], 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 bi-linearity 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 [109,110] 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. [111] 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 has been 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 auditing. This technique helps cloud clients to 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 is 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 [112].

Sharma et al. [113] 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 [114].

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 [115].

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. [116] 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 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 [117], 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 done on different sizes of data; encoding and decoding is also carried out for privacy purposes. Theoretical analyses and efficiency analyses are done 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 [118,119].

6. TPA-based security solutions and recommendation

We discussed in detail the following aspects in comparing the investigated approaches (depicted in Figure 7):

6.1. Comparison factors

6.1.1. Dynamic auditing

Based on our research (please refer to Figure 6, Table 2, and Table 3), the following were developed on the dynamic auditing factor:

- RSA-based storage security is utilized to recognize malicious cloud servers and to carry out dynamic operations. Yet, private keys, which are considered to be unsafe, are governed by TPAs.
- Cloud entities can be protected against Byzantine failures and colluding attacks by privacy negotiation mechanisms. Nevertheless, this mechanism can not assure users' data privacy.
- Privacy-preserving public auditing can be efficiently utilized by dynamic groups; however, this approach has high time-complexity and uses more bandwidth.
- Data privacy can be preserved by third-party storage audit services. This approach has decent communication cost. This approach utilizes dynamic operations; this thus affects the security of the used auditing protocol.

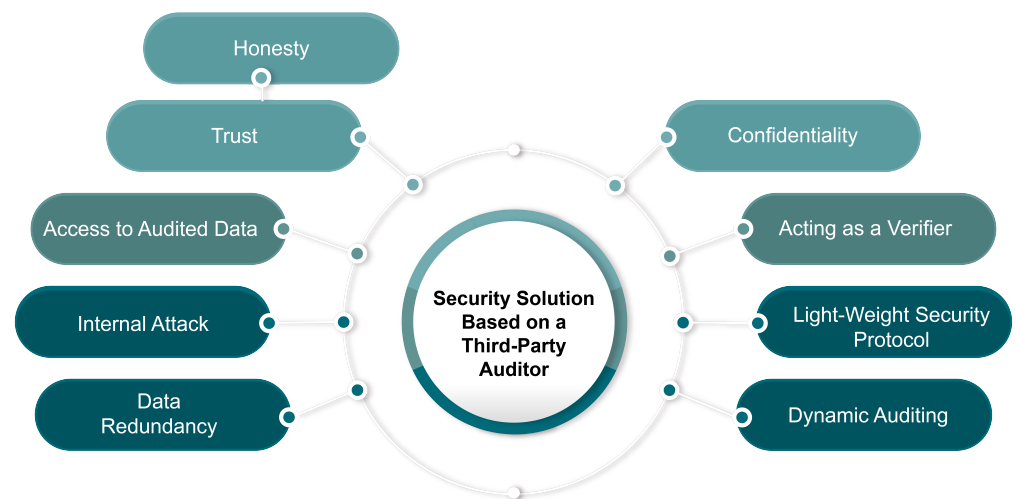


Figure 7. TPA Schemes Discussion.

6.1.2. Lightweight security

- Authentication and data confidentiality are ensured by the novel third-party auditor approach by utilizing encryption methods.
- Secret sharing and authentication can provide data privacy and mutual authentication between cloud service providers and cloud clients. Furthermore, utilizing secret sharing decreases cost of information exchange.
- The SCLPV is utilized to ensure secrecy if a large verification overhead is carried out. This technique can protect against malicious auditors.

6.1.3. TPA acting as a verifier

- The verifier should not be trusted if data privacy protection in the public cloud is the target.
- While performing the verification phase of the Knox and Oruta methods the data might be corrupted by adversaries.
- Reliability can significantly be improved by a designated public verifier. This technique can also decrease computation complexity.

6.2. Issues recurring from adopting a TPA

6.2.1. Trust

- The communication and computation costs are low when a public auditing mechanism is utilized. However, that internal attack might be a serious issue.
- Managing trust in TPAs could provide effective security protection. Nevertheless, this mechanism does not support cloud client feedback.
- Using encryption techniques can reduce computation costs and enhance data confidentiality.
- 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.

6.2.2. Access to audited data

- When the TPA applies random masking and homomorphic non-linear techniques, a decent efficiency will be achieved even if the TPA is carrying out various auditing tasks. Nevertheless, the TPA is able to obtain a local copy of the data.
- A data possession approach is utilized in cloud paradigms to provide decent anonymity.
- The layered interleaving approach can be employed during auditing to efficiently recover singleton losses. Nonetheless, data contents should not be exposed to the TPA.

6.2.3. Data redundancy

- The traffic cost is ideal when the PoOR approach is utilized. However, data redundancy might cause a serious issue.
- Trust could be established for cloud clients by the centralized trust model, however, feedback from cloud clients should not be completely trusted.

7. Conclusion

In this survey, cloud security based on a third-party auditor (TPA) has been 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; i.e., 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.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 research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Razaque, A., Jararweh, Y., Alotaibi, B., Alotaibi, M., Hariri, S. and Almiyani, M., 2021. Energy-efficient and secure mobile fog-based cloud for the Internet of Things. *Future Generation Computer Systems*.
2. Huang, Haiping, Xiang Sun, Fu Xiao, Peng Zhu, and Wenming Wang. Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. *Journal of Parallel and Distributed Computing* **2021**, 148, 46-57.
3. El Ghoubach, Imad, Rachid Ben Abbou, and Fatiha Mrabti. A secure and efficient remote data auditing scheme for cloud storage. *Journal of King Saud University-Computer and Information Sciences* **2019**.
4. Gudeme, Jaya Rao, Syamkumar Pasupuleti, and Ramesh Kandukuri. Certificateless Privacy Preserving Public Auditing for Dynamic Shared Data with Group User Revocation in Cloud Storage. *Journal of Parallel and Distributed Computing* **2011**.
5. Ibrahim, Fady AM, and Elsayed E. Hemayed. Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review. *Computers and Security*, **2019** 82 196-226.
6. Razaque, Abdul, Nikhileshwara Reddy Vennapusa, Nisargkumar Soni, and Guna Sree Janapati. Task scheduling in cloud computing. In *Systems, Applications and Technology Conference (LISAT) 2016 IEEE Long Island*. **2016**, 1-5. IEEE, .
7. Mohamed, Arwa, Mosab Hamdan, Suleman Khan, Ahmed Abdelaziz, Sharief F. Babiker, Muhammad Imran, and M. N. Marsono. *Software-defined networks for resource allocation in cloud computing: A survey*. *Computer Networks* **2021** 195 108151.
8. Yeh, Tsozen, and Yulin Chen. Improving the hybrid cloud performance through disk activity-aware data access. *Simulation Modelling Practice and Theory*, **2021**, 109 102296.
9. Xiao, Z. and Y. Xiao, Security and privacy in cloud computing. *Communications Surveys and Tutorials, IEEE*. **2012**, 15, (2), 843-859.
10. Li, M., Yu, S., Lou, W. and Hou, Y.T., **2012**, June. Toward privacy-assured cloud data services with flexible search functionalities. In *2012 32nd International Conference on Distributed Computing Systems Workshops* (pp. 466-470). IEEE.
11. Razaque, A., Li, Y., Liu, Q., Khan, M.J., Doulat, A., Almiyani, M. and Alflahat, A., **2018**, October. Enhanced Risk Minimization Framework for Cloud Computing Environment. In *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-7). IEEE.

12. Rajasoundaran, S., A. V. Prabu, Sidheswar Routray, SVN Santhosh Kumar, Prince Priya Malla, Suman Maloji, Amrit Mukherjee, and Uttam Ghosh. Machine Learning based Deep Job Exploration and Secure Transactions in Virtual Private Cloud Systems. *Computers and Security* **2021**: 102379.
13. Das, P., H. Classen, and R. Davé, Cyber-Security threats and privacy controls for cloud computing, emphasizing software as a service. *The Computer and Internet Lawyer* **2013** , 30, p. 20-24.
14. Kalluri, R.K. and Guru, C.V., **2021**. An effective analytics of third party auditing and Trust architectures for integrity in cloud environment. *Materials Today: Proceedings*.
15. Martucci, L.A., et al. Privacy, security and trust in cloud computing: the perspective of the telecommunication industry. in *Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing (UIC/ATC), 2012 9th International Conference on*. **2012**, IEEE.
16. Popović, K. and Ž. Hocenski. Cloud computing security issues and challenges. in *Proceedings of the 33rd International Convention*. **2010**, IEEEExplore, Opatija. .
17. Bowen, J.A., Cloud computing: Issues in data privacy/security and commercial considerations. *COMPUTER AND INTERNET LAWYER*. **2011**, 28, (8), p. 1-8.
18. Ryan, M.D., Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*. **2013**, 86(9): p. 2263-2268.
19. Krutz, Ronald L., and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. *Wiley Publishing*. **2010**.
20. Jansen, Wayne A. Cloud hooks: Security and privacy issues in cloud computing. In *2011 44th Hawaii International Conference on System Sciences* 1-10. IEEE, 2011.
21. Nithiavathy, R. Data integrity and data dynamics with secure storage service in cloud. in *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on*. **2013**, IEEE.
22. Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak. "Decentralized access control with anonymous authentication of data stored in clouds. *IEEE transactions on parallel and distributed systems*. **2014** 25, 2, 384-394.
23. AlZain, Mohammed A., Eric Pardede, Ben Soh, and James A. Thom. Cloud computing security: from single to multi-clouds. In *System Science (HICSS), 2012 45th Hawaii International Conference on*. **2012**, 5490-5499. IEEE.
24. Jhawar, Ravi, and Vincenzo Piuri. Fault tolerance and resilience in cloud computing environments. In *Computer and Information Security Handbook (Third Edition)* **2017** 165-181.
25. Patel A, Taghavi M, Bakhtiyari K, Júnior JC. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*. **2013**, 36, 1, 25-41.
26. Raghav I, Chhikara S, Hasteer N. Intrusion detection and prevention in cloud environment: A systematic review. *International Journal of Computer Applications*. **2013**, 68(24).
27. Modi, C.N. and Acha, K., 2017. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. *the Journal of Supercomputing*, **2017**, 73, 3, pp.1192-1234.
28. Shamshirband S, Fathi M, Chronopoulos AT, Montieri A, Palumbo F, Pescapè A. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*. **2020**, 55, 102582.
29. Kene SG, Theng DP. A review on intrusion detection techniques for cloud computing and security challenges. In *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, IEEE, **2015** , pp. 227-232
30. Paxton NC. Cloud security: a review of current issues and proposed solutions. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, IEEE, **2016**, pp. 452-455.
31. Manral, B., Somani, G., Choo, K.K.R., Conti, M. and Gaur, M.S., A systematic survey on cloud forensics challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)*, **2019**, 52, 6, pp.1-38.
32. Ru J, Yang Y, Grundy J, Keung J, Hao L. A systematic review of scheduling approaches on multi-tenancy cloud platforms. *Information and Software Technology*. **2020**, 106478.
33. A. Albugmi, M. O. Allassafi, R. Walters and G. Wills. Data security in cloud computing. *2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)*, **2016**, pp. 55-59, doi: 10.1109/FGCT.2016.7605062.
34. Shakarami A, Ghobaei-Arani M, Shahidinejad A, Masdari M, Shakarami H. Data replication schemes in cloud computing: a survey. *Cluster Computing*. **2021**, 1-35.
35. Domingo-Ferrer, J., Farras, O., Ribes-González, J. and Sánchez, D., Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. *Computer Communications*, **2019**, 140, pp.38-60.
36. Karthiban K, Smys S. Privacy preserving approaches in cloud computing. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, IEEE, **2018**, pp. 462-467
37. Chen, B., et al. Remote data checking for network coding-based distributed storage systems. in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*. **2010**, ACM.
38. Kaur, J. and J. Singh, Monitoring Data Integrity while using TPA in Cloud Environment. *Global Journal of Computer Science and Technology*. **2013**, 13 (3).
39. Chaczko, Zenon, Venkatesh Mahadevan, Shahrzad Aslanzadeh, and Christopher Mcdermid. Availability and load balancing in cloud computing. In *International Conference on Computer and Software Modeling, Singapore*. **2011**, vol. 14.

40. Wilson, K.S. and M.A. Kiy, Some fundamental cybersecurity concepts. *IEEE Access* **2014** 2 p. 116-124.
41. Eludiora, Safiriyu, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, and Lawrence Kehinde. A user identity management protocol for cloud computing paradigm. *International Journal of Communications, Network and System Sciences*. **2011** 4, 03, 152.
42. Gonzalez, Nelson Mimura, Marco Antônio Torrez Rojas, Marcos Vinícius Maciel da Silva, Fernando Redígolo, Tereza Cristina Melo de Brito Carvalho, Charles Christian Miers, Mats Naslund, and Abu Shohel Ahmed. A framework for authentication and authorization credentials in cloud computing. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*. **2013**, 509-516, IEEE.
43. López-Fernández, Luis, Micael Gallego, Boni García, David Fernández-López, and Francisco Javier López. Authentication, authorization, and accounting in webrtc paas infrastructures: The case of kurento. *IEEE Internet Computing*. **2014**, 18, 6, 34-40.
44. Behl, Akhil, and Kanika Behl. Security paradigms for cloud computing. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on*. **2012**, 200-205. IEEE.
45. Ko, Ryan KL, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, and Bu Sung Lee. TrustCloud A framework for accountability and trust in cloud computing. In *Services (SERVICES), 2011 IEEE World Congress on*. **2011**, 584-588, IEEE.
58. Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., & Attia, R. (2020). Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds. *Journal of Parallel and Distributed Computing*, 135, 1-20.
47. Xiao, Zhifeng, and Yang Xiao. Security and privacy in cloud computing. *IEEE Communications Surveys and Tutorials*. **2013**, 15, 2, 843-859.
48. Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Procedia Engineering* **2011**, 15, 2852-2856.
49. Hwang, G.H., Huang, W.S., Peng, J.Z. and Lin, Y.W., **2016**. Fulfilling mutual nonrepudiation for cloud storage. *Concurrency and Computation: Practice and Experience*, 28(3), pp.583-599.
50. Perez-Botero, Diego, Jakub Szefer, and Ruby B. Lee. Characterizing hypervisor vulnerabilities in cloud computing servers. In *Proceedings of the 2013 international workshop on Security in cloud computing*. **2013**, 3-10. ACM.
51. Sabahi, F. Cloud computing security threats and responses. in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. **2011**, IEEE.
52. Razaque, A., Amsaad, F., Hariri, S., Almasri, M., Rizvi, S.S. and Frej, M.B.H., **2020**. Enhanced grey risk assessment model for support of cloud service provider. *IEEE Access*, 8, 80812-80826.
53. Razaque, A., Nadimpalli, S.S.V., Vommina, S., Atukuri, D.K., Reddy, D.N., Anne, P., Vegi, D. and Mallapu, V.S., **2016**, March. Secure data sharing in multi-clouds. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1909-1913). IEEE.
54. Dunne, N.J., Brennan, N.M. and Kirwan, C.E., **2021**. Impression management and Big Four auditors: Scrutiny at a public inquiry. *Accounting, Organizations and Society*, 88, p.101170.
55. Beau, P. and Jerman, L., **2021**. Bonding forged in "auditing hell": The emotional qualities of Big Four auditors. *Critical Perspectives on Accounting*, p.102356.
56. Downar, B., Ernstberger, J. and Koch, C., **2021**. Determinants and consequences of auditor dyad formation at the top level of audit teams. *Accounting, Organizations and Society*, 89, p.101156.
57. Rizvi, S., Ryoo, J., Liu, Y., Zazworsky, D. and Cappeta, A., **2014**, May. A centralized trust model approach for cloud computing. In *2014 23rd Wireless and Optical Communication Conference (WOCC)* (pp. 1-6). IEEE.
58. Belguith, S., Kaaniche, N., Laurent, M., Jemai, A. and Attia, R., **2020**. Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds. *Journal of Parallel and Distributed Computing*, 135, pp.1-20.
59. Popovic, K. and Hocenski, Ž., **2010**, May. Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE.
60. Noor, Talal H, Quan Z. Sheng, Lina Yao, Schahram Dustdar, and Anne HH Ngu, CloudArmor Supporting reputation-based trust management for cloud services. *IEEE transactions on parallel and distributed systems*, **2016**, 27, 2, 367-380.
61. Kumari, Disuja, Karan Singh, and Manisha Manjul. Performance evaluation of sybil attack in cyber physical system. *Procedia Computer Science*. **2020**, 167, 1013-1027.
62. Wang, D., et al. Towards robust and effective trust management for security: A survey. in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* **2014**, IEEE.
63. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. and Vasilakos, A.V., Security and privacy for storage and computation in cloud computing. *Information Sciences*. **2014**, 258, p. 371-386.
64. Hussien, Z.A., et al. Public auditing for secure data storage in cloud through a third-party auditor using modern ciphertext in *Information Assurance and Security (IAS), 2015 11th International Conference on* **2015**, IEEE.
65. Cong Wang, Q.W., and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. In *2010 proceedings ieee infocom*. **2010**, 1-9.
66. Anbuchelian, S., Sowmya, C.M. and Ramesh, C., **2019**. Efficient and secure auditing scheme for privacy preserving data storage in cloud. *Cluster Computing*, 22(4), pp.9767-9775.

67. Pavithra S, Thangadurai E, Mailsamy M., Secure Data Storage in Cloud using Code Regeneration and public audition. *International Journal of Emerging Technology in Computer Science and Electronics (IJETCSE)* **2016**.
68. Worku, S.G., et al., Secure and efficient privacy-preserving public auditing scheme for cloud storage. *Computers and Electrical Engineering* **2014**, 40, p. 1703-1713.
69. Gajendra BP, Singh VK, Sujeet M. Achieving cloud security using third party auditor, MD5 and identity-based encryption. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*. **2016** 1304-1309, IEEE.
70. Yang, Kan, and Xiaohua Jia. An efficient and secure dynamic auditing protocol for data storage in cloud computing. *IEEE transactions on parallel and distributed systems*. **2012**, 24,9, 1717-1726.
71. Moghaddam FF, Karimi O, Alrashdan MT. A comparative study of applying real-time encryption in cloud computing environments. In *2013 IEEE 2nd International Conference on Cloud Networking (CloudNet)*. **2013**, 185-189, IEEE.
72. Kundu, Nibedita, Sumit Kumar Debnath, and Dheerendra Mishra. A secure and efficient group signature scheme based on multivariate public key cryptography. *Journal of Information Security and Applications*, **2021**, 85, 102776.
73. Wang, Boyang, Hui Li, and Ming Li. Privacy-preserving public auditing for shared cloud data supporting group dynamics. in *2013 IEEE International Conference on Communications (ICC)* **2013**. IEEE.
74. Wang, Q., et al., Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE transactions on parallel and distributed systems*. **2011**, 22, (5), p. 847-859.
75. Wu, T.Y., Lin, Y., Wang, K.H., Chen, C.M., Pan, J.S. and Wu, M.E. Comments on a privacy preserving public auditing mechanism for shared cloud data. in *Proceedings of the 4th Multidisciplinary International Social Networks Conference on ZZZ* **2017**. ACM.
76. Rizvi, S., A. Razaque, and K. Cover. Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment. in *Cyber Security and Cloud Computing (CSCloud)*, 2015 *IEEE 2nd International Conference on*. **2015** IEEE.
77. Razaque, A. and S.S. Rizvi, Privacy preserving model: a new scheme for auditing cloud stakeholders. *Journal of Cloud Computing* **2017**, 6, p. 7.
78. Rizvi, S., A. Razaque, and K. Cover. Cloud Data Integrity Using a Designated Public Verifier. in *High Performance Computing and Communications (HPCC)*, 2015 *IEEE 7th International Symposium on Cyberspace Safety and Security (CSS)* 2015 *IEEE 12th International Conference on Embedded Software and Systems (ICSS)* 2015 *IEEE 17th International Conference on*. **2015**, IEEE.
79. Ren, Y., Yang, Z., Wang, J. and Fang, L. Attributed Based Provable Data Possession in Public Cloud Storage. in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2014 *Tenth International Conference on* **2014**, IEEE.
80. Hao, Z. and N. Yu. A multiple-replica remote data possession checking protocol with public verifiability. In *2010 second international symposium on data, privacy, and E-commerce* **2010**, IEEE.
81. Erway, C.C., et al., Dynamic provable data possession. *ACM Transactions on Information and System Security (TISSEC)* **2015**, 17(4), p. 15.
82. Shrinivas, D., Privacy-preserving public auditing in cloud storage security. *International Journal of computer science nad Information Technologies* **2011** 2, (6), p. 2691-2693.
83. Wang, C., Wang, Q., Ren, K. and Lou, W. Privacy-preserving public auditing for data storage security in cloud computing. in *INFOCOM, 2010 Proceedings IEEE*. **2010**, Ieee.
84. Shen, W., Yu, J., Xia, H., Zhang, H., Lu, X. and Hao, R. Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third-party medium. *Journal of Network and Computer Applications*. **2017**, 82, p. 56-64.
85. Venkatesh, M., M. Sumalatha, and C. SelvaKumar. Improving public auditability, data possession in data storage security for cloud computing. in *Recent Trends In Information Technology (ICRTIT)*, 2012 *International Conference on*. **2012**, IEEE.
86. Jianhong, Z. and C. Hua. Secuirty storage in the cloud computing: a rsa-based assumption data integrity check without original data. in *Educational and Information Technology (ICEIT)*, 2010 *International Conference on*. **2010** IEEE.
87. Han, S. and J. Xing. Ensuring data storage security through a novel third party auditor scheme in cloud computing. in *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*. **2011**, IEEE.
88. Liu, Yanxiao, Chingnung Yang, Yichuan Wang, Lei Zhu, and Wenjiang Ji. Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. *Information Sciences*, **018**, 453, 21-29.
89. Kumaresan, R., A. Patra, and C.P. Rangan. The round complexity of verifiable secret sharing: The statistical case. in *International Conference on the Theory and Application of Cryptology and Information Security*. **2010**, Springer.
90. Yang, Ching-Nung, and Jia-Bin Lai. Protecting data privacy and security for cloud computing based on secret sharing. in *Biometrics and Security Technologies (ISBAST)*, 2013 *International Symposium on*. **2013**, IEEE.
91. Du, Ruiying, Lan Deng, Jing Chen, Kun He, and Minghui Zheng. Proofs of ownership and retrievability in cloud storage. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, **2014** pp. 328-335. IEEE.
92. Shacham, H. and B. Waters. Compact proofs of retrievability. in *International Conference on the Theory and Application of Cryptology and Information Security*. **2008**, Springer.
93. Yuan, J. and S. Yu. Proofs of retrievability with public verifiability and constant communication cost in cloud. in *Proceedings of the 2013 international workshop on Security in cloud computing*. **2013**, ACM.
94. Zheng, Q. and S. Xu. Secure and efficient proof of storage with deduplication. in *Proceedings of the second ACM conference on Data and Application Security and Privacy* **2012**, ACM.
95. Li, J., Tan, X., Chen, X., Wong, D.S. and Xhafa, F. OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices. *Cloud Computing, IEEE Transactions on* **2015** 3(2) p. 195-205.

96. Xiong, H., et al. Towards end-to-end secure content storage and delivery with public cloud. in *Proceedings of the second ACM conference on Data and Application Security and Privacy* 2012. ACM.
97. Zheng, Q. and S. Xu. Fair and dynamic proofs of retrievability. in *Proceedings of the first ACM conference on Data and application security and privacy* 2011 ACM.
98. Zhang, Y., Xu, C., Yu, S., Li, H. and Zhang, X, SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors. *IEEE Transactions on Computational Social Systems* 2015 2, (4): p. 159-170.
99. Li, H., Lin, X., Yang, H., Liang, X., Lu, R. and Shen, X, EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. *IEEE Transactions on Parallel and Distributed Systems* 2014 25, (8), p. 2053-2064.
100. Semwal, M.P., M.P. Tripathi, and M.H. Sharma, Enhance Data Security in Cloud Computing using Layered Interleaving Approach. *Journal of Global Research Computer Science and Technology*, 2015.
101. Singh, R., S. Kumar, and S.K. Agrahari, Ensuring Data Storage Security in Cloud Computing. *IOSR Journal of Engineering* 2012 2 p. 12.
102. Ke, C., Z. Huang, and M. Tang, Supporting negotiation mechanism privacy authority method in cloud computing. *Knowledge-Based Systems*. 2013 5 p. 48-59.
103. Syam Kumar, P., R. Subramanian, and D. Thamizh Selvam. Ensuring data storage security in cloud computing using Sobol Sequence. in *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*. 2010 IEEE.
104. Zhang, Y., Pan, J., Qi, L., and He, Q. (2021). Privacy-preserving quality prediction for edge-based IoT services. *Future Generation Computer Systems*, 2021 114, 336-348.
105. Huang, K., et al., Securing the cloud storage audit service: defending against frame and collude attacks of third-party auditor. *Communications. IET*, 2014. 8, (12), p. 2106-2113.
106. Xu, J., Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage. *IACR Cryptology ePrint Archive*. 2011, p. 304.
107. Huang, Longxia, Gongxuan Zhang, and Anmin Fu. Privacy-preserving public auditing for non-manager group. In *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1-6. IEEE.
108. Yu, Yong, Lei Niu, Guomin Yang, Yi Mu, and Willy Susilo. On the security of auditing mechanisms for secure cloud storage. *Future Generation Computer Systems* 2014, 30, 127-132.
109. Wang, B., B. Li, and H. Li. Knox: privacy-preserving auditing for shared data with large groups in the cloud. in *International Conference on Applied Cryptography and Network Security* 2012 Springer.
110. Yang, K. and X. Jia, TSAS: Third-Party Storage Auditing Service, in *Security for Cloud Storage Systems*. 2014, Springer. p. 7-37.
111. Zhu, Y., et al. Dynamic audit services for integrity verification of outsourced storages in clouds. in *Proceedings of the 2011 ACM Symposium on Applied Computing*. 2011, ACM.
112. Girma, Anteneh, Moses Garuba, and Jiang Li. Analysis of Security Vulnerabilities of Cloud Computing Environment Service Models and Its Main Characteristics. In *Information Technology-New Generations (ITNG), 2015 12th International Conference on*. 2015, 206-211. IEEE.
113. Sharma, Neha, Sanjay Tyagi, and Swati Atri. A Survey on Heuristic Approach for Task Scheduling in Cloud Computing. *International Journal of Advanced Research in Computer Science* 2017, 8, 3.
114. Shimbre, N. and P. Deshpande. Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. in *Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on*. 2015, IEEE.
115. Varalakshmi, P. and H. Deventhiran. Integrity checking for cloud environment using encryption algorithm. in *Recent Trends in Information Technology (ICRTIT), 2012 International Conference on*. 2012, IEEE.
116. Kaur, M. and M. Mahajan, using encryption algorithms to enhance the data security in cloud computing. *International Journal of Communication and Computer Technologies*. 2013, 1, (12): p. 56-59.
117. Suresh, K. and K. Prasad, Security issues and Security algorithms in Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering* 2012 2.
118. Akbari, Elham, Francis Cung, Hardik Patel, Abdul Razaque, and Hemin Nilesh Dalal. Incorporation of weighted linear prediction technique and M/M/1 Queuing Theory for improving energy efficiency of Cloud computing datacenters. In *Systems, Applications and Technology Conference (LISAT), 2016 IEEE Long Island*. 2016, 1-5. IEEE.
119. Wang, T., et al., A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing. *IEEE Transactions on Emerging Topics in Computational Intelligence*. 2018, 2, (1), 3-12.
120. Ben Haj Frej, M., Light-Weight Accountable Privacy Preserving Protocol in Cloud Computing Based on a Third-Party Auditor. *Doctoral dissertation*. 2020.