Journal of Engineering Science and Technology Review 14 (1) (2021) 1 - 24

JOURNAL OF
Engineering Science
and Technology Review

www.jestr.org

Review Article

Comprehensive Survey of Security Issues & Framework in Data-Centric Cloud Applications

Sudakshina Mandal* **and Danish Ali Khan**

Department of Computer Applications, National Institute of Technology, Jamshedpur

Received 19 March 2020; Accepted 16 February 2021

Abstract

The emergence of the cloud computing paradigm has influenced business organizations for migration over two decades. This has enabled a more incredible communication speed paired with a better fault tolerance of web-based applications and the scope of having practically unlimited storage available for the user and business data. Such colossal data availability over cloud platforms has increased concerns about the security of the same from various threats such as unauthorized eavesdropping, deliberate malicious mutation of data, loss of data integrity, and identity theft. The presence of such security vulnerabilities has rendered cloud security to be an active research area. This article aims to deep dive into the present state-of-the-art in cloud security research and mitigation approaches. It is observed that cloud storage, cloud services are the widely used applications among the organization. However, vulnerabilities and security challenges faced by this two area is maximum. Besides, outsourcing sensitive information to cloud service provider's (CSP) end leads to trust issues among organizations. This article performs a detailed comparative analysis of the security frameworks developed towards cloud storage level, cloud service level, and cloud trust level to date and throws light on future research directives. All the existing research has been evaluated against CIA (confidentiality, Integrity, Availability) principles here.

Keywords: Cloud Computing Survey; Cloud Security; Systematic literature review; Risk mitigation; Future in Cloud Security

1. Introduction

Over the year's cloud computing has got widely accepted by organizations as well as the individual. Cloud computing provides a centralized storage space along with a robust computation facility with a high-speed network [1]. The exiting features of platform-independent centralized space for resources with availability in reduced bandwidth makes the cloud more convenient [2]. This nature makes the cloud is ubiquitous. Numerous applications can be used over the cloud with high performance on a pay-per-use basis. This diverse quality of the cloud makes an attractive choice for the organization to shift their business. As this platform deals with numerous high computing resources and valuable information, ensuing security is one of the cloud's primary objectives. Different security protocol has been used by the Cloud Service Provider (CSP) for security preservation [3]. Easy access of applications over the cloud paradigm makes the industry more robust and provides ease of access. When using the cloud, it is not needed to deploy the individual application on the user's end. Organizations want a fair amount of storage space and user-specified applications with reduced cost according to their need [4].

Cloud storage usually consists of vast storage space with high computing server machines with the efficient network coverage [5]. Being equipped with several valuable resources with availability makes the cloud prone to security threats. Preserving security in cloud computing has a new trend in research currently. Presently, individual Cloud Service Provider (CSP) maintains a stringent security policy for data privacy over a secure medium. However, cloud computing faces vulnerability and several attacks that violate data privacy and make the resources unavailable due to threats' evolving nature. These security challenges degrade the shift to the cloud in an organization.

Cloud deals with sensitive data sources. Numerous security challenges and their countermeasures have been found from the research [6]. As the threats change their natures, the attack always found a new way to violate the resources. This article discusses security challenges and their preventive measures in three significant areas: cloud storage, cloud service, and cloud trust level [7].

The expansion of the digital era creates an increasing demand for storage space with network utilities. A cost-effective storage solution with high network capacity with lower bandwidth is the best choice for the business [8]. Data sources outsource their sensitive information to cloud storage over the secured network communication; after outsourcing data, sources lose control over the data. Following the Cloud Service Provider (CSP) 's stringent security policies, recent security attacks do not keep the researchers' look away. Apart from providing storage space, Cloud Service Provider (CSP) provides configurable pools of shared application which can use by the customer. These services can be software, virtual machine, hypervisor, storage space, and so on. These offerings reduce the capital expenditure of the business significantly by migrating to the cloud paradigm. The positive effect of using cloud applications is the flexibility and scalability of their nature. However, as an adverse effect, these applications' uses make the resources prone to privacy breaches. Cloud does not reveal the complex architecture nor their security protocol. When a customer uses the cloud

*E-mail address: sudakshina184@gmail.com

ISSN: 1791-2377 © 2021 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.141.01

service, they are not aware of the stringent security policy of the Cloud Service Provider (CSP). This violates the resources in danger and breaches integrity. Different Security threats have been discussed in the article depending upon the service [9].

In the above section, we talked about data-at-rest of cloud paradigm and security protocol of Cloud Service Provider (CSP). However, some other actors played a significant role in security challenges. The organization is always looking for a trusted solution for their licit purpose. Decision-makers take these roles on behalf of the organization and choose a suitable option for their business purpose. That third-party decision-maker can be harmful too. The malicious activity comes from the "trusted" cloud also [10].

This article will discuss the recent security challenges and existing preventive measurements in cloud storage, cloud service, and cloud trust level. Cloud storage and cloud service are the most useful features of cloud computing. So the investigation of these two areas with the detailed survey will be needful and beneficial. Trust factors influence the enterprise to choose appropriate cloud providers according to the need and specifications with an apt cost factor. Despite the importance of these two areas, a lack of transparency to ensure trust leads to severe data loss. The purpose of this article is to comprehensively review the mechanism, approaches, and state-of-the-art methods and study the background of these three area as mentioned above. This systematic literature review will provide a comprehensive literature review of the area as mentioned above. Individual existing work has been evaluated over their essential criteria and CIA (confidentiality, Integrity, Availability) characteristics. Authentication and authorization issues have been checked in regards to the trust level of cloud computing. The significant contribution of the article is given below

- This systematic literature review is focused on the cloud storage, service, and trust level.
- A detailed systematic literature review illustrates the process of this review.
- The particular area is highlighted with some significant security issues and existing state-of-the-art to mitigate those vulnerabilities.
- A tabular comparative analysis chart exhibits the security principles maintained by the existing research.
- Discussion of preventive measurement by analysis of the literature.

The rest of the article is organized as follows. **Section 2** will cover the brief of systematic literature review (SLR) and article selection procedure based on SLR. **Section 3** will give a detailed literature survey based on cloud storage level, service level, and trust level. A comparative analysis will be provided to compare the trends of mitigation techniques proposed so far. **Section 4** describes the current trends based on the analysis of the security principles and future research directives driven from the literature survey. **Section 5** draws the conclusion.

2. Systematic Literature Review (SLR)

Conducting research is a very daunting process. Research can be of two types one is primary, and another is secondary. In the primary research, data gathered directly from the research subject and required ethical approval. Secondary research is conducted with the existing data because it does not generate new data or interacts with humans or any subjects and does not need any ethical approval. A systematic literature review (SLR) is one of the research methodologies used to conduct secondary research. A systematic literature review (SLR) is different from a traditional literature review. A literature review is a synthesis of the summary of research, what has been done, identifies research gaps in the proposed field, and highlights what past research tells. A systematic literature review provides a purposeful and intentional selection of data that will be needful for the research study. It a process in which a body of literature is collected, reviewed and assessed with pre-specified techniques. The goal is to identify a clearly defined problem with existing evidence and scope of the research work done with some further research questions which will be concluded any research gap of research, any recommendation, any questions, any contradictions, any findings, any further research proposals [11], [12] [13]

a. Life Cycle of Systematic Literature Review (SLR)

The process of performing a systematic literature review includes the following stages (Figure 1) reported in an original research article with the same name [14].

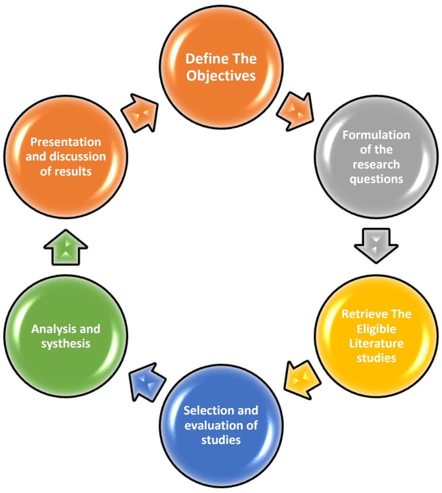
Define The Objectives
Formulation of the research questions
Retrieve The Eligible Literature studies
Selection and evaluation of studies
Analysis and synthesis
Presentation and discussion of results

Fig. 1. Life Cycle of Systematic Literature Review (SLR) [32]

Step 1: Define The Objectives:

The first step of a systematic literature review (SLR) is to define the objectives. So, Identifying the objective and significance of this systematic literature review (SLR) is the initial step here. The objective must specify the needfulness of this review and future perspective [11]. According to the specified objective, articles should be chosen, which is elaborated in the next part.

This article aims to scrutinize the security loopholes of cloud storage, service level, and trust level from the existing research and depict the effectiveness of those research towards the CIA (Confidentiality, Integrity, Availability) principle along with two extra parameter privacy and recovery. This article also aims to classify the security loopholes, analyze the mitigation technique, and study the security parameters [15].

Step 2: Formulation of the research questions:

The second step is to formulate the research questions that follow the objectives. By analyzing the existing research, this section proposed some technical questions. This article highlights those concerns and identifies the research gap in those existing research [16].

Following technical questions according to the goals are discussed in this article [14] [17].

The above questions represent in table 1 are evaluated against the selected article. The article selection process is described in the following section. We aim to analyze the current research trends with RQ1 to preserve security in industry structure. The trend is analyzed based on the chosen criteria such as cloud storage level, service, and trust level security. In RQ2, proposed frameworks have been scrutinized to evaluate the contribution towards security goals. With RQ3, different techniques identify and check their relevance, where RQ4 identifies the security principle followed by the proposed work. Different security attack prevention is structured from the existing articles and evaluated in RQ5 [18].

Table 1. Research questions as per criteria

ID	Research Questions	Rationale
RQ1	What are the approaches enterprises have taken to ensure security?	Identify the trend of security protocol used to ensure privacy and security on the relevant criteria proposed earlier in the article
RQ2	Contribution of the existing approaches to ensure security parameters?	Scrutinize how the existing work ensures security. The process is evaluated against several security principals
RQ3	Techniques adhere to propose a framework	Identify the methodology used for the proposal of the framework
RQ4	Security principles (CIA) followed by the existing framework	Analyzing the security principal CIA (Confidentiality, Integrity, Availability) followed or not
RQ5	What are the different security attacks which can be prevented from the existing literature	Evaluation of the proposed work against several security threats

Step 3: Retrieval of the significant Literature studies

This step involves finding the appropriate journal by searching for different electronic repositories. Identifying the electronic database and specified time period is necessary for the retrieval of literature. The article must be selected based on the keywords relevant to the research objective. Selected articles followed below steps for synthesis of the review [19]. In this article, we will choose articles regarding the issues of storage level, Trust level, and service level and provide a guideline of the current research position, the methodologies used so far, why this review is necessary, and what questions to be answered [11].

Step 4: Selection and evaluation of studies

In this stage, evaluation is done based on significant characteristics. Parameters need to be identified for evaluation of the articles. Selected articles from the previous stage are analyzed in-depth based on the specified criteria. Significant articles have been chosen here by maintaining the similarity of the research context [1].

In this article , the article selected based on cloud storage level, service level, and trust level is analyzed, and irrelevant research has been discarded.

Step 5: Analysis and Synthesis

Analysis and synthesis have been performed based on the criteria proposed in step 4. Here, articles are arranged according to their publication year. Evaluate the strength, weakness, robustness of existing frameworks along with their probable future directives.

In this article existing mitigation frameworks and loopholes have been synthesized and analysed. Based on this, a comparative table should be prepared to mention the research methodology taken based on key research areas [14].

Step 6: Presentation and discussion of results

This stage deals with the discussion and the results of the review. Comprehensive diagrams and charts have been prepared for data representation. The significance of this review is discussed , and comparative analysis with existing research has also been discussed. A detailed analysis report has been produced based on the security challenges and mitigation methods proposed in existing research in a stipulated time period. According to the drawbacks, this article presents some guidelines for future work. Future directives also discuss the collaboration of blockchain, edge computing, and big data for ensuring security and privacy.

b. Article Selection Procedures

The article selection procedure has been discussed here. This procedure deals with significant steps. Each step is discussed here with the below-mentioned table.

The article selection procedure starts with selecting the electronic database first. The database used in this systematic literature review (SLR) includes ScienceDirect-Elsevier, IEEE Explore, Springer, Wiley, and ACM digital library. The majority of the articles have been taken from the ScienceDirect-Elsevier, IEEE Xplore, and Springer database. The time frame was chosen as 2012- 2019 for the article selection procedure. Here Table 2 represents the collection of the electronic database with their URL [12]. Keywords are applied to search for the compatible research work in the above-mentioned electronic database systematically. All the keywords have been chosen based on two criteria. The first criteria are based on the research question and the second criteria are the specified area chosen for this article. All relevant articles have been chosen based on the specified topic as cloud storage, cloud service level, and cloud trust level security. Keywords that are applied to the electronic database will be combined using Boolean “AND” and “OR.”. Table 3 determines the collection of keywords used to search in the database. Based on the keywords, articles have been chosen for further processing. Articles are comprised of the journal, conference proceedings (International and national) , book chapters. The strategy adopted for shortlisting is described below. Table 4 presents the tabular details of the number of selected articles in each stage from the electronic databases. The first column of table 4 represents the name of the electronic database used for article selection. Column 2 to column 4 are the representation of individual steps. Numbers signify the aggregation of article selected in each stage. Following steps (Steps 1-4) are followed for choosing the appropriate article.

Step 1: Select the articles based on the keywords from the electronic databases. It is observed from Table 4 is that a total of 124 articles is selected in this stage.
Step2: From the selected article retrieved from step 1, we need to analyze and eliminate the article which is irrelevant to our research topic. A total of 107 articles have been shortlisted from 124 articles from step 1 for this article and exclude the rest.

Step 3: Exclude irrelevant articles based on abstract and conclusion content based on the searched keywords. Stage 3 choose 84 articles among 107 articles according to the criteria.
Step 4: This is the final stage. Here articles chosen from step 3 are analyzed based on the article topic, research questions, and suitable contents. 84 Articles coming from step 3 are analyzed based on specified criteria, and 65 articles are chosen for final review.

Table 2. Electronic databases used in SLR.

Online Database	URL
ScienceDirect-Elsevier	http://www.sciencedirect.com/
Springer	http://link.springer.com/
IEEE Xplore	http://ieeexplore.ieee.org/
ACM digital library	http://dl.acm.org/
Wiley	http://www.onlinelibrary.wiley.com/

Table 3. Keywords use in SLR

Keywords Used
Cloud Computing Security
Cloud computing security Review
Systematic Literature Review
Security in cloud storage
Security in Cloud Service
Security in Cloud trust
threats in cloud computing
Cloud security future

Table 4. Number of Articles as per electronic databases

No.	Electronic Database	Step 1	Step 2	Step 3	Step 4
1	ScienceDirect-Elsevier	40	31	28	24
2	Springer	22	20	17	14
3	IEEE Xplore	40	36	24	13
4	ACM digital library	10	10	7	6
5	Wiley	12	10	8	8
	Total	**124**	**107**	**84**	**65**

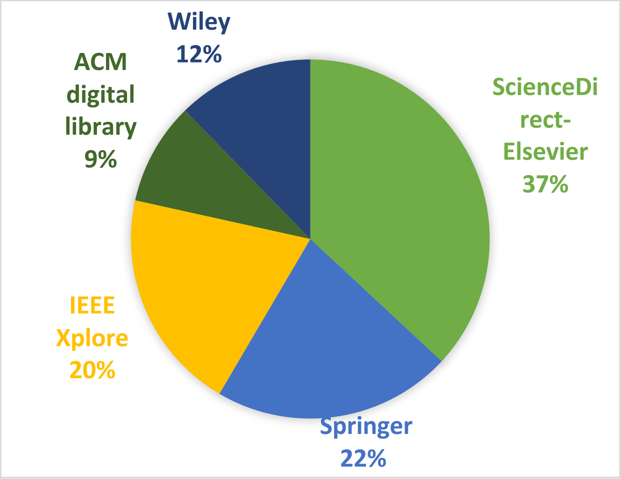

Fig. 2. Distribution of article in the final stage (Stage 4)

The distribution of selected articles in the final stage is represented in figure 2 in percentage. Based on Figure 2, it is observed that most of the articles are taken from the ScienceDirect-Elsevier database, Springer, and IEEE Xplore databases in the final stage. International and national journals, conferences, book chapters are evaluated against different criteria. In the final stage, all relevant articles have been checked based on two criteria, i.e., research article and review article. We got the summarized snapshot of the current research work on that current period from the review articles. Some critical articles have been found for better analyzed which is described in the next section. From the research articles, individual research works are analyzed for suitableness.

Figure 3 exhibits the number of article selection graph in the stipulated time frame used for this article. Figure 3 shows the blue bar represents the year, and the green curve represents the number of articles chosen for this article. It is visible from the graph that, among 65 articles in the final stage, the number of the article has the maximum count in the years 2016 and 2017. We have taken the time frame from 2012 to 2019 for our systematic literature review (SLR).

3. Finding of Security Aspect and discussion of threats According to the objectives

According to the latest trends and nature of the threats, we categorized the security challenges into three broad perspectives: cloud storage level security issues, Cloud service-level security issues, and cloud trust level security issues. Being the most used application, cloud storage and cloud services are prone to more eavesdropping attacks compared to others. Apart from cloud storage, cloud services are diversified into three categories, namely software-as-a-service (SaaS), platform-as-a-service (PaaS) , and infrastructure-as-a-service (IaaS). These three categories cover extensive applications starting from web application to virtualization. When an organization renders cloud service from the cloud service provider (CSP), choosing an appropriate cloud is taken by any third-party decision-maker on behalf of the organization, leading to trust issues. Firstly, end users are not aware of the security principals or protocols and organization does not thoroughly know the stringent security policy adheres by cloud service providers (CSP). By using this advantage, attackers break the integrity of cloud service. Violation of SLA (Service level agreement), Auditing issues are also accounted in trust issues. As the use of cloud increases associated by different other technologies like artificial intelligence, machine learning, deep learning, IoT , security breaches are also increases in the same matter. Extensive research has been done to mitigate those problems. However, the evolving nature of threats cannot be prevented anyhow, which gives the organization second thought of outsourcing their data to the cloud.

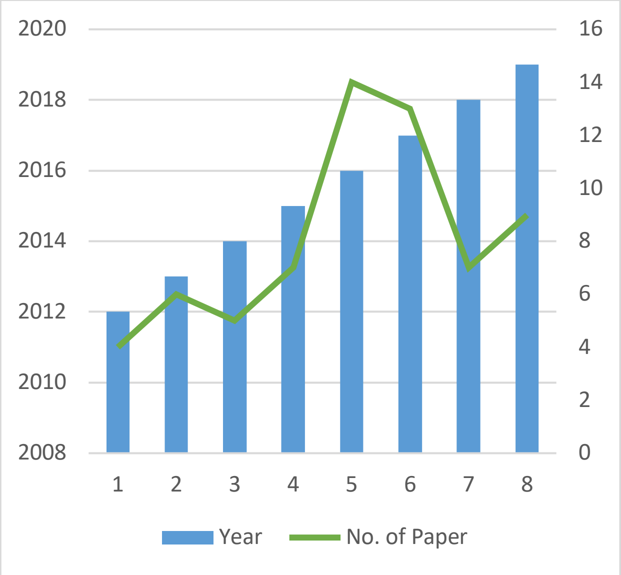

Fig. 3. The number of the article selected in step 4 between 2012-2019

Based on the above security challenges, in this section, we will discuss the latest security attacks in these three major categories and will state the findings from the articles of rigorous literature survey [20]. Each category are described in the following subsections.

3.1 Cloud Storage Level

The enterprises are transformed towards cloud storage due to the reduced cost, data availability, security, and agility over two decades. The need to use the cloud with this transformation is accelerated exponentially day by day. Cloud storage is the first choice for the organization currently [20, 21]. There are four types of cloud storage, namely public cloud storage, private cloud storage, Hybrid cloud storage, and personal cloud storage. The use of cloud storage is not limited to organizations, but it is widely used by individuals also. Cloud Data storage assembled many data storage spaces together through the application software, which is based on the functions of the cluster applications, grid techniques, distributed file systems, and so on. A third-party cloud service provider (CSP) provides cloud storage with pay per use with rapid scalability. This storage will be accessed via web services API [22]. After outsourcing data to the cloud storage, data owner loses their control from the sensitive information. This information can be used from the dispersed location by multiple clients. This information faces significant security loopholes. Attackers penetrate the cloud storage by stealing the authentication from the data owner and using those data for their licit purpose. Data breaches are not limited to penetrating the cloud by violating authentication data, it includes several access points and leads to significant data losses, which is discussed below.

3.1.1 Cloud Storage Architecture

Primarily cloud storage is used as a storage medium. Cloud storage maintains a business layer logic behind the application used by the data owner. It consists of a front end which exports the API for access to the business layer. This front end can be of several types, namely web service front end, file-based front end, Internet SCSI front end, and iSCSI front end. Behind this API, the middleware or business layer resides. This layer is responsible for various features like data replication, data reduction over traditional data replacement algorithm. The back end implements the physical storage space for the data [20, 23]. Figure 4 describes the diagrammatic view of cloud storage architecture.

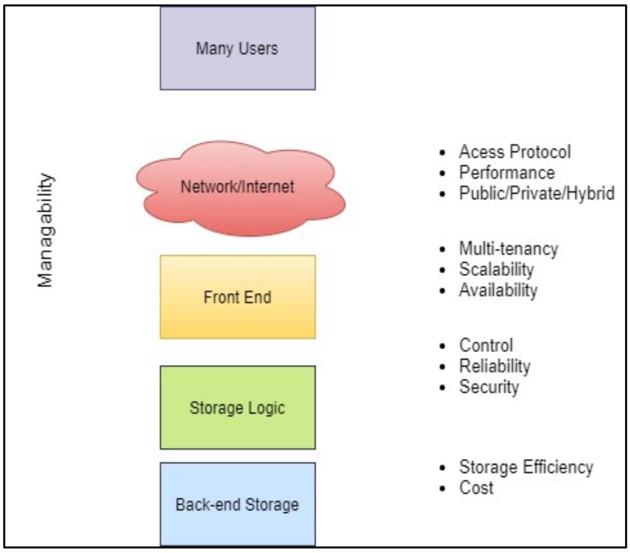

Fig. 4. Generic cloud storage architecture [24]

3.1.2 Cloud Storage Standards

Storage Network Industry Association (SNIA) published Cloud Data Management Interface (CDMI) to standardize the client's protocol, roles, and responsibilities with the enterprise. This holds up both the legacy and new applications. CDMI is used to create, delete, retrieve and update data in cloud storage [22]. This sets the protocol for standard remote data auditing by cloud service providers (CSP). With this standard's help, clients can quickly identify the responsibilities and capabilities of respective cloud storage offerings [25]. Cloud storage Providers (CSP), Cloud service users, Cloud service developers, cloud service auditors, cloud service brokers are the main actor for using this service [26].

3.1.3 Drawbacks of cloud storage

The significant drawbacks are illustrated in this section.

Security breaches: Security breaches is the most common drawback which hampers the integrity of the sensitive information stored in cloud storage. The cloud service provider (CSP) have stringent security policies for data protection. However, organizations do not deal with those policies, service level agreement (SLA). This endangers the risk of being exposed the sensitive information to a group of an unauthorized persons, or it might be stolen or viewed [22]. Collaborating with significant technology and scientific advancement makes the information prone to eavesdropping recently[27].

Limitation of Bandwidth: How much data can be transferred from one place to another in a specified time is known as bandwidth. The exponential growth of the data transfer rate might lower the bandwidth. Data bandwidth, network bandwidth , and digital bandwidth are the classifications of bandwidth. Loss bandwidth leads to severe data packet loss. These drawbacks could give space some illicit activity over network bandwidth, digital bandwidth [28].

Network Latency: Temporal propagation delay in transmitting the data packet within the network slower causes network latency. A slower network or any disruption in the network causes serious data issues to the cloud storage. Loss of data packet violates the integrity of the stored information. However, network can be used as a medium to penetrate into cloud storage for any unethical purpose [29].

Efficiency: Although cloud storage seems like a very efficient that gives fast data outsourcing, data processing and concurrent access. Collaborative with several new technologies like artificial intelligence, IoT, machine learning, natural language processing (NLP) makes the information more robust and efficient. However, sometimes complicated procedures, critical scientific calculations, and useful artificial intelligence tools for information analysis lead to inefficiency in concurrent access over stored information [30].

Accessibility issues: Accessibility issues cover authentication authorization issues. Without significant authentication, prior knowledge of service level agreement (SLA) sensitive information can easily be exposed by breaking the authentication and service policy for any licit purpose. Accessibility issues are also happened by unauthorized attackers. Authorization plays a significant role when accessing the stored information. Unauthorized persons have a bar to access that information outside of the organization. Different social engineering attacks, cybercrime has been employed to penetrate into the cloud storage by any unauthorized hacker [31].

3.1.4 Issues in Cloud Storage Level

Despite significant benefits, data sources face security challenges over the cloud storage. As the data is hosted in cloud , the data owner does not possess any access control to prevent the issues [23]. Over two decade's massive expansion of data growth escalates the use of cloud storage. Organizations or individuals can use cloud storage on pay per use basis, subscription basis etc. [32]. Apparently, the storage procedure seems safe, but the data that resides in storage are dynamic in nature, which endanger the security of sensitive information. Regular addition, deletion and concurrent access of information o leave the system in an inconsistent state where tradition security mechanism misses the loopholes. Some Issues are listed in following

Data Security Issues: Cloud storage security or data security is used interchangeably in a different context. When the data is transferred to cloud storage faces several attacks or security breaches. As the client has no control over the hosted data, data violation causes a massive problem in this context [33]. Several prevention schemes have been proposed so far to deal with data exposure with cryptography, steganography, etc., to conform to data confidentiality, integrity, and availability [5].

Loss of data control: As cloud storage provides low-cost, scalable, readily available storage space, the number of using cloud storage increases day by day. Apparently, cloud storage infrastructure looks exciting and straightforward to the client as they do not need to bother about the cloud provider's security principle or even the terms and conditions. When the data is stored on the third party's cloud space, the client loses control over their potential data. As cloud service needs to conform to the CIA (Confidentiality, Integrity, and Availability) triad of security principle, here loss of control violates this principle. If the data breaches occur at the service provider's site users, have no control over it. Sometimes it might have data provider outsource their data on scientific purpose or for purposeful service. With the loosing of control, the client's data might be prone to several data breaches [34].

Data duplication Problem: To gain more profit and to get more efficiency in storage, when an enterprise uses cloud storage for their employee it might happen similar copy of information has been sent by the employees, which incurred extra cost for the enterprise. According to the survey conducted by EMC, 75% of digital data gets duplicated [35]. So deduplication in cloud storage is happening very often [36]. Deduplication allows the storage to store a single copy of every piece of information. When a data owner uploads any information into the cloud storage, it first checks whether the hash value or the index of that particular file has already been stored or not. If the hash value has already been stored in the storage that means the connection with the file owner has already been established. Cloud storage deduplication saves the storage space, but it faces maximum security problems. As the storage is business-critical, it might happen unauthorized access for deduplication causes a severe problem[37].

Data Integrity Auditing Problem: Significant security challenges violate data integrity and hamper confidentiality. This causes a severe security problem. When the data is manipulated, deleted by the untrusted attacker in the cloud storage, it leads to data security issues. Different auditing schemes have been proposed to solve this problem and to possess the integrity of remote data in cloud storage. Significant public and private auditing techniques have been proposed so far for auditing [38]. Some existing integrity methods can only serve for statically archived data, and some auditing techniques can be used for the dynamically updated data. Most existing public auditing techniques have an assumption that the auditor will be an honest person and cannot temper the data. However, what is worse if a dishonest data auditor colludes the data and mislead the data owner by corrupted the private key or public shared by the data owner at the time of auditing [33]. Sometimes the client needs to employ their private key for data authentication in auditing schemes. So the user possesses a hardware token to store the private key. If the hardware token is lost or the password is forgotten, then auditing would not be performed, and security will be hampered [36].

Data Backup Issues: Data backup is essential for accidental and disaster recovery. For the availability of data, backup is a must for every cloud storage. Cloud service providers (CSP) regularly perform data backup by maintaining specific guidelines or protocols to prevent data tampering and any malicious activity. However, any person involving data backup can cause any severe insider attack problem and violets data. The user's email address or personal authentication information is shared for backup, which can be misused by any CSP's end [23]. Cloud service provider runs over the business body and runs their business over the revenue collected. If the revenue is not covered up, then there might be a chance of shutting down the business. If the clients have some issues with service providers and are if organizations might get reluctant to pay, then data security is also at stake[39].

Data Recovery Issues: Due to the nature of resource pooling, cloud storage gives the provision for the on-demand service of resources. Many users can use a similar resource at different points in time. If a memory or storage location is shared among several clients, it might happen a malicious client recovers the previous data by using the data recovery technique. This may cause a severe security issue. Apart from this third party, the cloud service provider (CSP) is employed to recover data from the client end if the system is corrupted or any technical issue. These third-party CSPs are also on the top list of where security breaches occur [23].

Inappropriate Media Refinement: Sometimes storage media needs to be sanitized for the following reasons which are, i) for the disk replacement, ii) the slaughter of service iii) no need to maintain the old disk. Sometimes these refinements cause significant security challenges over sensitive information. It is challenging to pertain data integrity and confidentiality at the time of refinement [23] as the cloud storage system maintains a multi-tenant structure. Loss of media, network latency is the major drawback for this cause.

Network Performance Issues: Cloud is entirely dependent on the network. The performance of accessing the cloud varies depending upon the network throughput and latency,. Despite the drastic improvement of network throughput, the performance is less compared to local network coverage. Cloud service providers (CSP) have been trying to increase the throughput by local caching. It depends upon the network data sharing and data backup that takes place. Several threat attacks, intrusion attacks cause a security problem by violating confidentiality, integrity, availability of stored data [20].

Not understanding the service level agreement (SLA) : The Service Level Agreement (SLA) is a contract that is signed between the client and the cloud service provider (CSP) about the function and non-functional requirements of the cloud service. SLA considers obligations, service pricing, and penalties in case of agreement infringement. When clients outsource their data to cloud storage, they do not have proper awareness of the SLA agreement's terms and conditions. In most cases, clients have no idea how storage space is hosted in multi-cloud storage (MCS) manner [5]. The dishonest cloud service provider can take this chance to violate and temper the data and breach privacy, integrity, availability of the hosted data[40].

Abstract Nature of Cloud: Cloud computing features make a lucrative choice for the organization. Cloud features reduce the overhead and complexity of organizations and individuals drastically. However, this does not seems to be very easy. The process does not limit to outsourcing and hosting over cloud storage. Each vendor has different storage procedures, access methods, standards and protocols, APIs, etc. some cloud service providers (CSP) give the provision to the client to implement standard network file sharing protocols such as Network File System (NFS) or Common Internet File System (CIFS) [41]. The lack of interoperability and control over cloud storage makes it difficult in data migration [20].

3.1.5. Exploring State-of-the-art of cloud storage

Several security measures have been taken up by the cloud service providers (CSP) depending upon the cloud storage type and architecture. Different security preservation models proposed as countermeasures of different cloud security attacks occur based on the sensitive information. To ensure data protection, a significant proposal has been adopted, which will be applicable not only for cloud service providers (CSP), it is also applicable for organizations and individuals. Data protection novel methodology has been proposed to secure the authentication problem and cybersecurity problem related to cloud storage. Some recent works in the stipulated time period have been discussed in this section based on their strength and efficiency in table 5.

Table 5. State-of-the-art of cloud storage models

Article name	Proposed Scheme	Strength	Efficiency
Security and privacy in cloud computing[42]	Scheme to secure resident data	i) Protect user structured, unstructured data. Ii)Discussed the protection of virtual machines & cloud computing services	Suggested that the decentralized cloud system is the best solution for storing large scale unstructured data (Big Data)
Cloud security issues and challenges: a survey [7]	Presented a survey on the security issues and challenges in cloud computing	A well-defined, comprehensive table of recent cloud attacks and threats makes the article more appropriate.	Performance is evaluated for each security solutions
Secure overlay cloud storage with access control and assured deletion [43]	File Assured Deletion (FADE) protocol, a secure overlay cloud storage system to achieve fine-grained, policy-based access	i) Symmetric &asymmetric key used for encryption. This technique is based on ABE algorithm re-encryption. It supports data	No

	control and file assured deletion.	sharing with access control policy	
Security and privacy for storage and computation in cloud computing [44]	SecCloud, a privacy cheating discouragement to provides storage security on computational data, auditing using encryption	This scheme verifies the data location. Merkle hash tree is employed to ensure computational security.	No
Integrity Audit of Shared Cloud Data with Identity Tracking [45]	A secure and practical scheme for a dynamic group of client	To track the data identity tracking, addition deletion of clients, this scheme added a new role called Rights Distribution Centre (RDC).	Defines a new audit model for shared data in cloud. Probable security theory helps to prove security in the proposed scheme
Secure Multi-Owner Data Storage With Enhanced TPA Auditing Scheme In Cloud Computing [46]	A privacy-preserving public auditing based on homomorphic linear authenticator and random masking.	Guarantee that the TPA would be ignorant about the data's content at the time of public auditing.	Comprehensive analysis and performance evaluations make the model more efficient
Intrusion Detection and Security Calculation in Industrial Cloud Storage based on an Improved Dynamic Immune Algorithm [47]	Improved dynamic immune algorithm to secure data in storage. Shift mutation for iNSA and random grouping for iDCS used for detector generation and dynamic update.	Protect cloud storage data from changeable network circumstances and detect intrusion attacks.	Experimental results show IDIA can detect the non-self-samples accurately and recognize self-samples with higher precisions. The experimental analysis makes the article more appropriate.
Public Integrity Auditing for Cloud Storage based on Consortium Blockchain [33]	A blockchain-based public integrity verification for cloud data storage	Proofs of Retrievability (POR) and Provable Data Possession (PDP allow a data owner or a third party auditor to verify the integrity of outsourced data without actually having them as private and public auditing.	i) It proves efficiency through performance analysis. ii) To reduce computational time burden, a blockchain-based scheme consortium public integrity verification (CBPIV) is proposed.
Data Integrity Auditing without Private Key Storage for Secure Cloud Storage [48]	data integrity auditing scheme is proposed by using biometric data as users fuzzy data without using private key storage	new signature scheme is proposed to support blockless verifiability and which compatible with the linear sketch	Efficiency and robustness proved by performance analysis. To check computational and communication overhead, they compared their proposed scheme with Shacham and Waters's scheme
Secure and economical multi-cloud storage policy with NSGA-II-C [49]	A solution based on multi-cloud storage. Non-dominated Sorting Genetic Algorithm II with a unique process of Combinations (NSGA-II-C)	This is the first work to propose an index to measure the security degree of MCS policy. It transforms the security degree in MCS into MOP	Comparison with several MCS schemes and performance analyses proves the efficiency of the technique. The performances of NSGA-II-C, MOEA/D , and SPEA2 are compared to solve the formed MOP.
A Dynamic Programming Approach to Secure User Image Data in Cloud Based ERP Systems [50]	A map-based data hiding scheme(LCS based) is proposed using steganography	It store the mapping of cover-secret image. Thus it is difficult for the attacker to retrieve the original text. This scheme is used mainly to prevent insider attack in cloud storage	i) Cantor pairing is used to decrypting at recipient's end. ii) Performance analysis also produced empirical analysis. Iii)reduce storage space, cost increase efficiency
Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment [51]	time-based proxy re-encryption (TimePRE) approach	Allows the user's access right to expire automatically after a predetermined period.	No
New approach for ensuring cloud computing security: using data hiding methods	A new approach to ensure security by using encryption and watermarking tool.	i)Experimental results prove the approach is secure enough.	i) Stegdetect is used to check the robustness

[52]		ii) Whatever the data capacity and the content, data hiding methods used as a factor to enhance the security	ii)Performance analysis proves the efficiency
Research on data security technology based on cloud storage [53]	Data secure storage scheme based on Tornado codes (DSBT) to support efficient data loss recovery ability, effectively resist the Byzantine fault	computational efficiency of POR algorithm is optimized	System performance-tested here. It introduces the implementation of DSBT system based on trusted log and POR system
A New Security Framework for Cloud Data [54]	The security framework is proposed based on a genetic algorithm(crossover and mutation)	i)The concept of the key is not present in the framework, which increases security ii) It uses a capability list to ensure fine-grain control access	It reduces the computation time by using GA and increase the performance
A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications [55]	A Chinese Remainder Theorem (CRT)-based privacy-preserving data storage mechanism to store the user data in the cloud database	New formulas have been taken for encryption and decryption. Ceaser cipher encryption scheme is used for key generation	Experimental results show the performance is better than other models.
An Autonomous Security Storage Solution for Data-Intensive Cooperative Cloud Computing [39]	The autonomous storage security model is proposed to increase trust	Superposition of complex security policies and overcoming the mistrust between the users and the platform	Security storage service can be easily integrated into the cooperative cloud computing environment. A prototype model is prepared to check efficiency.
One Quantifiable Security Evaluation Model for Cloud Computing Platform [56]	Quantifiable security evaluation model to be applicable for any type of cloud system and accessed by consistent API.	This method consists of evaluation criteria comprises of several fields in storage, network, maintenance and many more in cloud.	Implementation is done on G-Cloud platform to provide dynamic security scanning score for one or multiple clouds with visual graphs and guided users to modify the configuration, improve operation, and repair vulnerabilities
Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage [57]	Decentralized efficient multi-authority attribute-based scheme for mobile data storage	Key escrow problem is removed by evaluating trust on data owner. It minimizes computational overhead, encryption; decryption speed is an increase,	Performance evaluation is done based on online or offline cloud data sharing protocol on both cloud data owner and cloud data user. Proof–of–concept also implement to show the system is efficient.
A highly efficient algorithm towards optimal data storage and regeneration cost in multiple clouds [38]	Provenance Candidates Elimination (PCE) algorithm to investigate trade-off problem of resource utilization	Running time is reduced compared to the GT-CSB algorithm. It is scalable if the dataset is extensive.	Efficient in finding minimum strategy of cost in data storage, transfer, regeneration.

3.1.6 Comparative analysis of the state-of-the-art of cloud data storage

A detailed, comprehensive analysis is presented in this section. This analysis is based on different parameters that can cover all significant aspects of the techniques under consideration. All the methodologies have been evaluated against confidentiality, integrity and availability (CIA) principles. Besides it analyze the privacy and recoverability factors from the methods. The articles selected in the final stage for cloud storage security have been scrutinized for this cause and the following table is represented accordingly in table 5. The first column corresponds to the article reference and the second is indicating the year of publication. Column 3-7 represents security parameter.***Yes*** is marked if a proposed model conforms to a parameter, and a ***No*** is marked if the model does not enforce the particular parameter. If a article does not discuss any security principle and does not ensure, ***NA*** (Not applicable**)** is put in the table 6.

Table 6. Comprehensive analysis of the security principles of cloud storage

Author Name	Year of publication	Confidentiality	Integrity	Availability	Privacy	Recovery
Z. Tari [42]	2014	Yes	Yes	Yes	No	NA
Singh et. Al [7]	2016	Yes	Yes	Yes	No	NA
Y. Tang et al. [43]	2012	Yes	Yes	NA	Yes	NA
Wei et al. [44]	2014	Yes	Yes	Yes	No	NA
Yan et al. [45]	2019	No	No	No	Yes	NA
Nandini. J et al. [46]	2014	No	Yes	No	No	NA
Wang et al. [47]	2018	NA	NA	NA	NA	NA
Lin [33]	2019	No	Yes	No	No	NA
Shen et al. [48]	2018	NA	Yes	NA	NA	NA
Yang et al [49]	2019	NA	NA	NA	NA	NA
Mandal et al [50]	2019	Yes	NA	NA	Yes	Yes
Liu et al. [51]	2014	NA	NA	NA	NA	NA
M Yesilyurt et al. [52]	2016	Yes	Yes	Yes	NA	NA
R Wang et al. [53]	2017	Yes	NA	Yes	NA	Yes
Shalu Mall et al. [54]	2018	Yes	NA	Yes	NA	NA
Prabhu et al. [55]	2019	No	No	No	Yes	No
Jiang et al. [39]	2013	NA	NA	NA	NA	NA
Sun et al. [56]	2018	No	No	Yes	No	Yes
Sandor et al. [57]	2019	Yes	No	No	Yes	No
Zhang et al. [58]	2019	NA	NA	NA	NA	NA

NA* = Not Applicable

3.2 What is Cloud Service-based Application?

Cloud services are intended to provide scalable, easy access to the application, services, and resources managed by the cloud service providers (CSP) [39] over the internet. Cloud services can scale to fulfill consumers' requirements dynamically according to the need and provide the service's hardware and software. The term service is also used to describe professional services that support the selection, management, and deployment of various cloud resources. Cloud services currently include online access to the application software, storing data in storage, data backup, email services, document collaboration[59].

3.2.1 Classification of Cloud Services

The Cloud holds the concept of software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In the concept of cloud, everything is available through services like storage-as-a-service, trust-as-a-service, security-as-service, and XaaS (Anything as a service). However, apart from the traditional concept of "service", there exists a concept of professional services and web services [60].

3.2.1.1 Cloud Service vs. Professional Service

Professional services allow consumers to deploy different types of cloud services. Consulting firms, systems integrators, and other channel partners may offer such services to help their clients for the adoption of cloud-based technology [61].

Somewhere cloud services are synonymous with web service or application-based service. Though they are interlinked, these are not identical. In the cloud, a web service provides a platform for applications to communicate through WWW. Consumers use the applications through the web and use the product. Applications as a service refer to the delivery of software applications as a service over the Internet. Application service is termed to provide software to enterprise consumers more efficiently because it can be distributed and maintained for all users at a single point in the public cloud (Internet) [62]. In this section, the application-based services or web services will be discussed.

Nowadays, application-based service uses are maximum in the cloud domain. As the new technologies and vast amounts of data are incorporated daily, the loopholes and security threats have become more prominent. This service level faces authentication authorization problems, data security problems, access control, trust-based problems, etc [63].

3.2.2 Application-level Security Issues

Over the internet, cloud-based applications are consumed extensively across organizations [60]. SSL/TLS protocols protect the web browser of applications for authentications and security reasons[64]. The attacker could have hampered authentications by penetrating several threats and getting access to the other user's XML token to affect the browser [63]. Some significant attacks are discussed, which affect the application level most. The security challenges do not limit to the above issues. As cloud services are composed of multiple technologies, attackers can penetrate the service in several ways. Here in this section we will discuss application level security issues only. In other words we can say application-level cloud services or web-based cloud services are more prone to security breaches and leads the data in a vulnerable state. Apart from the hardware-based cloud services, these services are more accessible to the user, thus this is the primary target for the attacker for breaching. Plenty of research has been proposed to ensure and protect information , but collaborating with significant technologies makes the breaches easy and critical to detect. Some of the well-known attacks are discussed in this section here.

SQL injections attack: To exploit the regular system database and to gain access to the potential user's information saved in the database such as username, password, bank details, the attacker injects malicious SQL command and penetrate sensitive information and hampers integrity of data [65]. The injection can happen over a weak network or session hijacking. This attack works silently. When an organization runs that specific operation , the SQL code will disrupt the system and breaks the data integrity.

Cookie Poisoning: Generally web browsers stored the search history and cookie at the consumer's end. Any search history can be found in the future by utilizing the cookie. Hijacking any particular data owner by impersonifying, it can be easy to hijack cookies. Forging a cookie by the attacker is known as cookie poisoning. As consumers' potential credentials are stored on a cookie, manipulating a cookie can be an unauthorized attacker's access point. The search history can be useful data for any illicit activity for the hacker[66].

Backdoor and debug options: Applications may have a backdoor at the time of development or debug. After making the application deployable to the cloud, sometimes, backdoors are opened to ease out the programmer[67]. Attackers take advantage of the backdoor by making it an entry point and damage sensitive information. Security breaches can also be happened if any insider is malicious. The use of backdoor and disrupt the system will be an easy task for them[68].

Hidden field manipulation: Some hidden fields are embedded in some applications or websites containing some confidential information, mainly used by the developer for internal communication between browser and server. Due to inadequate coding nature, sometimes those fields are susceptible to hackers and intruders [69].

Google Hacking: Nowadays, Google is used as the best common phenomena search engine. To find some potential information about some users, Google is the best way for hackers to probe a system. Hackers try to break the security by finding loopholes in the system. After collecting potential information, hackers intrude on the system and disrupt the system [70].

Man in the middle attack: A significant attack on SSL where malicious hacker acts as an Intermediary person between a conversation and client-server communication. They impersonate the conversations to gain access and steal the potential information to back the malicious information to each other [71, 72].

CAPTCHA Breaking: CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), also called Human Interactive Proofs (HIP) , was developed as a security mechanism for the protection of computer resources, used by several web sites like Microsoft, Google, Yahoo [73]. CAPTCHA is used to prevent the re-registration of website spammer as it is difficult to break the CAPTCHA easily. However, Artificial Intelligence, Pattern Recognition, image processing, computer vision, and many others technology are used to break the CAPTCHA and violate computer resources' integrity [73].

Intrusion Attack: Unauthorized access of computer resources and potential information that violates the integrity is known as an Intrusion attack where the attacker can attack in the application layer, transport layer, and network layer [74]. Several Intrusion Detection systems are designed to monitor data traffic, recognizing any harmful actions [9].

Social Engineering Attack: Malicious activities perform through human interactions where psychological manipulation is used to trick the user into making any security mistakes or giving away sensitive information to the attacker. This attack is the most common technique of hacking nowadays. Significant technologies have been used to trick the user [75].

Steganography attacks: The attacker embeds some malicious code into a file transmitted over the network, which may be ignored by the system's security mechanism and acts as a standard file to the user [9]. When these embedded or extracted bits perform in steganography or the receiver decodes the bit string using their key , the attacker gets the key by this process.

Web services & protocol based attack: Various protocols such as SOAP are used by web services whose message header can be altered and inject invalid request by hackers to hamper the message's consistency [9].

3.2.3. Authentication and access control level security issues

Authentication is a process by which validating and guaranteeing is done of users, which is the principal means of protecting resources over cloud applications [76]. Breaches of Access control and user authentication make the security principles at stake [77]. Some of the significant authentication breaches are:

Password Guessing Attack: It includes several attacks by obtaining the potential user's password. Breaking password is very easy for the attackers. Double password protection has been employed for authentication [78] [79].

Replay Attack: Here, the attacker identifies the authentication packet of data and injects malicious code and reproduces a new packet in an unauthorized way [80].

Masquerade Attack: This attacker pretends to be the user and gain the privilege [81].

Insider Attack: It also refers to injecting some malicious code like Trojan horses and penetrating sensitive information and affecting security. Insider attack signifies when an insider person in the organization disrupts the cloud system. As the insiders have particular authentication and access control to the cloud application. It can be effortless to affect the cloud and use this information for unauthorized activity. Security attack happens by the insider is challenging to detect always [82].

Phishing Attack: This is one of the significant types of social engineering attacks, which attempts to steal us[83]ername, password, etc. in various ways by providing fake emails and fake websites to the consumers. Currently significant software and techniques have been employed over the web browser to monitor any targeted consumer's activity. Monitoring will give the history of the consumers' interest. By provoking them with their choice of interest, they become the prey of phishing attacks. Phishing has been taken over the cybersecurity world and research has been employed for mitigation [84].

Shoulder Surfing Attack: This is another type of social engineering attack where an attacker steals personal identification and authentications such as user id and password by looking over their shoulder or hijacking the access [85].

3.2.4 Exploring State-of-the-art of cloud Service Based Application

In this section existing frameworks (qualitative and quantitative) have been discussed, which are already in use to prevent security threats. A comprehensive table of the strength and robustness of those frameworks is proposed here in table 7. Each article is evaluated based on the strength and robustness of the security principle.

Robustness: The extent to which the proposed method shows resilience to the change in the adversary threat model

Strength: Advantages and features of the proposed approach.

Weakness: Drawbacks of the approach

Table 7. State-of-the-art of cloud service models

Article Name	Proposed Framework	Strength	Robustness
Security problems in cloud computing environments: A deep analysis and a secure framework [86]	Multi-dimensional Mean failure cost model (M^2FC)	i)Security problems are analyzed according to security requirements ii) Keeps privacy	Risk is calculated in accordance with financial loss per unit operation time
Toward Authorization as a Service ,A study of the XACML standard [87]	service by adopting XACML(Extensible Access Control Markup Language) standards	i)Have self-contained policies ii) Minimize cost iii) Can be extended by a reusable component iii) Adaptability with the heterogeneous system.	Feasibility tested in OSGi platform
A Security Framework In Cloud Computing Infrastructure [88]	Approaches will work as Security-As-A-Service	Ensures security principles that ensure the least bandwidth, computational cost, fewer resources etc.	The best mechanism is chosen According to experimental analysis for cross security issues
Multilevel classification of security concerns in cloud computing [89]	Dynamic Security Contract (DSC)	i) Cost-benefit analysis is performed. ii) MAX(SLA) & MIN (penalties) for CSP can be achieved once the max and min costs for countermeasure are known	Risk is calculated according to the intensity
New approach for ensuring cloud computing security: using data hiding methods [52]	Based on Encryption and watermarking	i) Enhance security and easy to extend ii) Fewer resources consumption iii) Protect data from copyright	The experimental survey was conducted to assess the approach
Towards quantification and evaluation of security of Cloud Service Providers [69]	Used GQM paradigm to quantify performance & propose an evaluation methodology	i)transparent ii)Can be deployed on any third-party site	The case study is producing over IaaS cloud providers
Security as a Service for Public Cloud Tenants(SaaS) [59]	Used IDS based framework (uses signature and anomaly detection techniques)	i)Tenant can protect their virtual private network ii) Works as security as a service (pay as you go)	Calculated percentage of CPU consumption of the LIDS compared to the FLIDS
Towards performance evaluation of cloud service providers for cloud data security [90]	Proposed data security models based on Business Process Modelling Notations (BPMN) to analyze performance issues	BPMN helps to understand the potential breaches & helps to recover from it ii)Allows organizations to review the system	Authentication & Identification proves the efficiency

Research on data security technology based on cloud storage [53]	A data secure storage scheme based on Tornado codes (DSBT)	Enhance the quality and computational efficiency	i)Strong data loss recovery ii) Using the DSBT scheme, computation efficiency is optimized
Homomorphic Encryption for Security of Cloud Data [91]	Homomorphic encryption is used to store data	Simple and efficient	No
Security-by-design in multi-cloud applications: An optimization approach [92]	Adopted graph-based Multi-cloud Application Composition Model (MACM)	)Improve security and reduce development costs ii)Develop secure and cost-effective applications iii)Improve the optimal deployment problem	Performance is evaluated in terms of memory and CPU usage, cost
Security assurance assessment methodology for hybrid clouds [93]	Security assessment methodology	i)Scalable ii)Provide a better assessment result to the CSP's and the users	Performance is evaluated in terms of several security parameters
Block Design-based Key Agreement for Group Data Sharing in Cloud Computing [94]	A block design-based key agreement protocol	i) Supports multiple participants to share the outsourced data with high security and efficiency freely iii) Provide safety and reliability.	i)Secured against active and passive attack ii) Performance evaluation is given
Lightweight IoT-based authentication scheme in cloud computing circumstance [95]	lightweight crypto-modules like one-way hash function and exclusive-or operation are adopted	i)Secured against several attacks	i)Robustness is guaranteed ii)Performance and computational cost is evaluated by comparison
Generating stable biometric keys for flexible cloud computing authentication using finger vein [77]	Bio-key generation algorithm named FVHS,	i)Stable ii)Reduce the number of the weak network key	Experimental analysis proves the robustness
A pervasive electroencephalography-based person authentication system for cloud environment [96]	Pervasive biometric authentication systems using Electroencephalography (EEG) signals	An innovative way evaluates user identification, authentication, verification. ii)detailed experimental results are produced	Performance is better than two existing approaches in terms of accuracy
Offering security diagnosis as a service for cloud SaaS applications [63]	Security Diagnosis as a Service (SDaaS) to analyze the security status Of SaaS applications and detect the threats	This method is compared with anomaly detector, penetration tester, code analyzers, generate a comprehensive report of security risks	evaluate the detection accuracy, performance, and scalability by experimental analysis
Design of cloud security in the EHR for Indian healthcare services [97]	The framework proposed to store health records by using a text-based encryption scheme.	Double data security provided by isolation between encryption schemes of transmitted data & stored data	The experimental analysis produced scalability of this method, which can be adaptable in a large population
Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes [98]	novel multi-layer cloud architectural model for the interaction of the heterogeneous IoT based devices	i) Ontology is used to solving the heterogeneity problems introduced in smart home services. ii) Backbone of a future	Well-known security attacked is prevented effectively here.

		smart home, which makes the standard of living high.	
Effects of security and privacy concerns on educational use of cloud services [99]	A research model is proposed to posit that student attitudes predicted by security and privacy perceptions and behavioral intentions	i) Survey questionnaires are formed to assess the model based on collected data. ii) Results show the intense significance of privacy and security principles.	No

3.2.5 Comparative analysis of the state-of-the-art of Cloud Service Based Application Level

Considering the contemporary techniques in the cloud service-based model from the literature in the above section, a comprehensive analysis of cloud security principles is introduced in this section in table 7. Confidentiality, Integrity, Availability, and Privacy are taken as parameters for evaluating security. ***Yes*** is marked if a proposed model conforms to a parameter, and a ***No*** is marked if the model does not enforce the particular parameter. If a article does not discuss any security principle and does not ensure, ***NA*** (Not applicable**)** is put in this table 8. The first column is represented as the article name. The second to the fifth column is represented as confidentiality, integrity, availability, privacy and authentication accordingly. This table will give the idea of which domain is mostly highlighted in existing research for ensuring security.

Table 8. Comprehensive analysis of the security principles of cloud service

Article Name	Confidentiality	Integrity	Availability	Privacy	Authentication
M Jouini et al. [86]	yes	yes	yes	NA	No
R Laborde et al. [87]	yes	yes	NA	NA	NA
A Ukil et al. [88]	yes	yes	NA	NA	yes
S.A Hussain et al. [89]	NA	NA	No	yes	yes
M Yesilyurt et al. [52]	yes	yes	yes	NA	NA
T. Halabi et al. [69]	NA	yes	No	NA	NA
M. Hawedi et al. [59]	NA	No	NA	NO	No
M Ramachandran et al. [90]	yes	yes	yes	yes	NA
R Wang et al. [53]	yes	yes	yes	NA	NA
M M Poteya et al. [91]	yes	NA	yes	NA	No
V Casola et al. [92]	NA	**yes**	yes	NA	yes
A Hudic et al. [93]	yes	yes	yes	NA	No
J Shen at al. [94]	NA	NA	No	NA	NA
L Zhou et al [95]	NA	No	NA	No	yes
Z Wu et al. [77]	Yes	NA	yes	NA	yes
P Kumar et al. [96]	NA	yes	No	NA	yes
Elsayed et al. [63]	yes	NA	yes	no	
Deshmukh et al. [97]	yes	yes	NA	NA	yes
Tao et al. [98]	yes	NA	NA	NA	No
Arpaci et al. [99]	NA	yes	NA	NA	yes

3.1 Cloud Trust level

The significance of trust and impact upon the cloud is described in this section [100]. Some recent research works have taken as a literature survey to look into the trends, and a comprehensive table is prepared whether those maintain the CIA principles or not.

3.3.1 What is trust in the cloud?

Trust consists of three things: belief, Expectation, and willingness to take risks [101]. Organizations uses cloud services from cloud service providers (CSP) in pay per use basis. Organizations select the appropriate cloud service based on the need and the uses with reduced cost. This decision has been taken by any third party. The organization put its trust in the third party for choosing the cloud service. Choosing the cloud service solely depends on the reputation, security policies, recoverability and many more cloud service features. Trust plays a significant role in this aspect [102]. By trusting the cloud service provider (CSP) organizations outsource their sensitive information to cloud applications. So ensuring trust is essential security feature. Breaches of trust lead to severe security challenges. This section will discuss the definition of trust, several security challenges found from the selected article chosen for the literature survey. A detailed analysis chart has been produced to demonstrate whether the proposed methods from the literature ensures security principal or not.

Trust is a measurement of the reputation of the cloud service provider (CSP) who provides resources for users. Trust plays an essential role in growing the cloud business and make more profit. As trust has no particular definition, some correlative definitions can be derived [103].

Definition1: Trust is considered as the recognition of an entity's identity, behavior, and confidence. As an entity's behavior depends on the experience gathered by them, the judgment of trust is subjective in nature [100].

Definition2: Trust value is used to calculate the level or degree of the entity's trust.

Definition3: Direct trust is when the entity is calculated the trust value by direct interaction.

Definition4: Recommended trust or indirect trust calculated from the third party who establishes a direct connection with the desired entity and evaluated trust.

3.3.2 Features of Trust

Trust can be classified by several features [103]. As trust has no direct definition to follow, these features strengthen the concept of trust. Some of the significant features are described below [104].

Asymmetry: If A and B have set up a trust relationship, the evaluated task calculated by A will be different from the calculated trust of B.

Subjective, uncertainty, and fuzzy: The nature of trust is very uncertain in nature and fuzzy.

Inconstancy and context-sensitive: The value of trust is changeable with time and context.

Condition-based transitivity*:* A's evaluated trust for B will be unequal to C's recommended trust.

3.3.3 Classification of Cloud Trust Model

The process of evaluation of system trust is called modeling of trust. Trust can be established in two ways. The first one will be an expected trust calculated from Trustor's end. The second one is based on the experience collected by the Trustor experience. The first type of trust model displays an unequal relationship from both ends. A trustor establishes trust according to the belief, performance, or behavior. A trustee will use the product provided by them with the level of belief, which will not match the trustor's trust [105]. The following diagram of figure 5 displays the classification of trust. We will present each section below.

Cloud Trust Model based on Performance: Cloud trust is established by collecting the record of a particular cloud service provider (CSP) [106]. Trust is established by calculating the performance metrics, service ranking of the cloud service provider. Trust is also calculated by checking the recoverability from security breaches, service efficiency , and many more significant criteria [107]. The relationship between trustor and trustee plays a significant role when evaluating trust [108].

The performance metrics can be considered by the following questions:

a) Is the service robust enough?
b) What is the fault tolerance rate?
c) How many users are connected?
d) Network tolerance level?

Cloud Trust Model based on Belief: Based on the trustor's belief, cloud trust can be established in this section. When a trustor establishes trust by belief, it is not guaranteed that the trustee can comply with that belief or not [106]. So when choosing a cloud model understanding between trustor and trustee is both important. Service efficiency is always essential as well as user-friendliness and ease of use [109].

Cloud Trust Model based on Behaviour: By taking the cloud service provider's (CSP) behavior, trust can also be established. By collecting a significant historical behavioral dataset a trust model is prepared through which trust can be achieved. This historical data includes significant parameters such as efficiency, ease of use, recoverability from any fault and many more [110].

Recommended Trust Model Recommendation has been made by choosing definite QoS parameters in the cloud. A significant standard has been followed to ensure QoS parameters for establishing recommendation. This model is one of the popular models where a recommendation has been chosen by any third-party organization on behalf of the original organization.[106]. This recommendation has been chosen by evaluating the need of the organization. The best chosen is selected depending upon the ranking of the cloud service. A significant mathematical model has been proposed for ensuring trust [111].

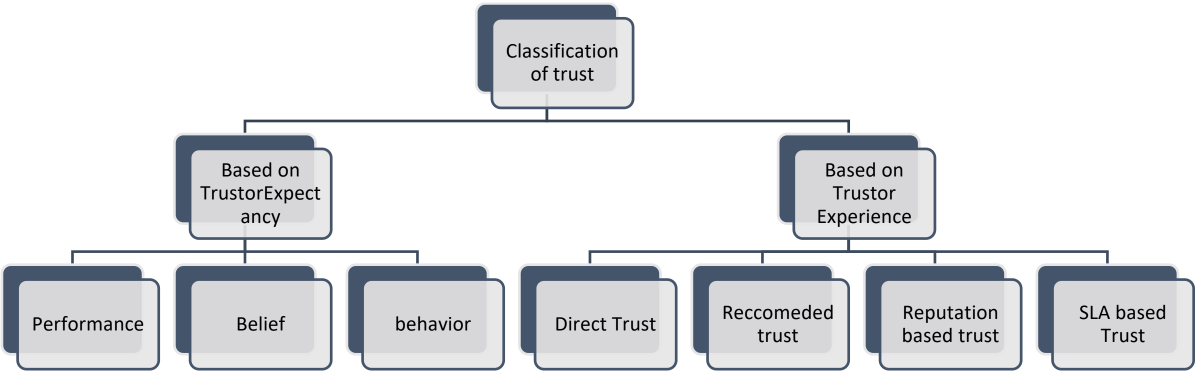

Fig. 5. Classification of Cloud Trust Model

Reputation-based trust Model: In this model, the third-party auditor chooses the cloud service model by collecting feedback and customers' opinion to measure the trust. Reputation is established by evaluating the significant QoS criteria to measure cloud trust. According to the ranking based on reputation, trust is established over a significant cloud service provider (CSP) [112]. In recent days this model gets the highest popularity among cloud service providers and consumers to make a cloud trust rank apart from the recommendation trust model. This model can quickly provide the appropriate ranking by calculating QoS parameters and historical feedbacks [110].

Service level agreement (SLA) Based Trust Model: In this type of trust model, trust is decided based on the service agreement and contracts between cloud service providers and cloud consumers. Service level agreements (SLA) and service policy reports are the most frequently used QoS criteria [113]. By evaluating the appropriate criteria suitable to measure service level agreement, the cloud service provider (CSP) has been chosen. Standard trust model has been followed like recommendation model, reputation model to choose the CSP based on service level agreement (SLA) [114].

3.3.4 Parameters for Trust Evaluation

As the concept of trust is asymmetric, fuzzy, and subjective in nature, there are no such predefined parameters exist to evaluate trust. Different authors proposed significant parameters to calculate the trust factor. Some of the trust factors are discussed below. After evaluating the existing trust model for ensuring security from the literature it is found that, Grandison et al. [115] identified that trust could be composed of numerous significant parameters. These are also called QoS parameters. To evaluate trust significant criteria among several QoS parameter has been chosen. Some of the criteria are reliability, honesty, security, availability, integrity, completeness, timeliness, turnaround efficiency, return on investment (ROI) , dependability etc. a few are discussed below [116].

Availability: In software engineering, availability is calculated by measuring the mean time between failures and the meantime to repair time. The unavailability issue might be happening for the following reasons [116]: a) Resource might be shut down. b) Any part of the resources might be denied to the user. C) Resource pool can be busy to serve a request. Let , assume that R_1, R_2 … R_m are the cloud resources. For each k = 1, 2 … m, let N_k denote the number of jobs submitted to cloud resource R_k over a period T. Out of N_k jobs submitted to R_k, let A_k denote the number of jobs accepted by the resource R_k over the period T. The following equation is calculi the availability for ensuring trust.

$$availability = \frac{A_k}{N_K}$$

Data Integrity: Data integrity is considered one of the significant parameters for calculating trust. Consider a total number of the job is C_k and the total number of resources is $R_{k.}$ Then, out of C_k jobs completed successfully by resource R_k, let D_k indicate that the number of jobs data integrity preserved by resource R_k over the period T. The following equation signifies the data integrity calculation [117]. Loss of sensitive information from the cloud breaches data integrity. Obsoleted infrastructure might cause data integrity breaches which violate trust from the cloud service providers (CSP)

$$Data\ Integrity = \frac{D_k}{C_K}$$

Turnaround Efficiency: The interval of time between submissions of a job to completion of a job is known as the turnaround time. Turnaround time cannot be predefined. It depends on the cloud service providers (CSP) [116]. If the turnaround time taken by the CSP is longer than the predefined turnaround efficiency it is calculated as 1. The calculation of finding turnaround efficiency (TE) is calculated below. Turnaround efficiency of a resource R_k (TE) is calculated as the average turnaround efficiency over all the jobs submitted during the period T [118].

$$turnaround\ efficiency = \frac{Promised\ turnaround\ time}{actual\ turnaround\ time}$$

3.3.5 Issues based on cloud trust

Selecting an appropriate cloud service provider (CSP) by pertaining trust is the objective of the organization. Previous reputation and ranking helped the consumers to choose the proper one for their business. Comprising any of the quality of service (QoS) of trust can be taken as a security breach. A better understanding between the cloud service provider (CSP) and cloud user is needed for establishing trust [119]. However, the reason for slowing down the up-gradation to cloud computing is the lack of guarantee and trust between the cloud service providers (CSP) and consumers. Many trust-related issues and challenges are faced by both parties (clients and providers), creating security breaches. Challenges can be from any other side (either from the client or from the providers). As trust can be considered the level of satisfaction or confidence, it is necessary to enhance the security and privacy factor [120]. Some of the challenges are discussed below.

Security: Security plays an essential role in building trust. Stringent security policies have been implemented on the cloud services by the cloud service providers (CSP) to ensure trust. Different authentication , authorization level agreements make the service more robust and reliable. Any security challenge makes the service at stake. Any vulnerable cloud service loses its reputation [121]. Apart from this most of the web cloud services are the first target for the cybersecurity attacker by personify, hijacking network, and many more. To build full trust, Cloud Service Provider (CSP) should maintain security compliance in virtual conditions such as control information leakage and network issues [122].

Lack of Control: Control is the primary issue related to trust. When the users lost their control over their assets, the system is considered less trusted. When a money transfer happens under a secured network connection is must be trusted. However, if a client deposits money outside the enterprise's control, they may face some trust issues [120].

Ownership: Ownership of the enterprise also guarantee trust. Trust plays a twofold relationship when an enterprise releases their application in the cloud. Cloud service providers must be confident about their security protocol and service level agreements (SLA) to gather trust, and from the client-side, they must comply with the trust of the cloud application which they have used [120].

Reputation: Online trust is also dependent on the cloud service provider's (CSP) reputation or brand value. By evaluating brand value or collecting user feedback, an enterprise builds a relationship with that company. Breaches of security or any violation affect their reputation and hamper trust [6, 123].

Reliability: The ability to perform a specific task or performance of a component under a situation in a specified period is known as reliability. Reliability is considered a failure-free operation at a specified time. The reliability parameter is calculated as follows [6]:

$$Reliability\ in\ time\ y = e^{-\lambda t}$$

$$\lambda = \frac{items\ failed}{total\ operating\ time}$$

Reliability is the most dependent factor for measuring trust. Breaches of reliability create a loophole in data security by which illicit hackers can penetrate the cloud system and break the trust.

Lack of transparency: When any client uses the cloud in an organization, they do not know much about the security policies, protocols provided by the third-party cloud service providers (CSP). The stringent security policies have not been transparent to the end-users. Consumers only outsource their data to the cloud. This lack of transparency puts the data in a vulnerable state which in turn puts the cloud in an untrusted state[110].

Apart from the client-side, the cloud server level might face several trust issues, such as Network failure, Database failure, Software management failure, Server (Hard-disk) failure [108]. To give protection in the cloud by traditional hard security mechanism cryptography, steganography, several authentications , and authorization techniques provide a concrete foundation, but it fails when it will need to give protection to the entities which are temporary, asymmetric, undefined. The incorporation of malicious entities in the cloud environment makes the risk of breaching trust. In private cloud computing, trust is at the highest level as the assets and infrastructures are managed by a privately well-known entity. The clients are from different enterprises in the community cloud, but they share a standard security mechanism protocol[120]. Thus the trust level is lesser than the private cloud comparatively, but it is better than the public cloud. The security breaches happen maximum in the public cloud as the communication entities , and the service level agreements (SLA) are unknown [10].

Trust issues can be divided into four categories, according to Kavitha et al. [121].

i) How to give the definition and evaluate trust following unique parameters in cloud environments?
ii) How to handle malevolent information when a trust relationship is dynamic and temporary?
iii) How to provide security service depending upon the security parameters?
iv) How to manage trust degree change with interaction time and context and monitor, adjust, and accurately reflect the trust relationship dynamic.

Keeping the similar track, we will dive into the literature and depict the proposed work that has ensured trust in the next section. The exploration will be noted in tabular format.

3.3.6 Exploring State-of-the-art of cloud Trust Models

Significant research has been done to ensure trust in the cloud. Different trust models have been studied in this article for the evaluation of trust. IT is clear from the literature that significant methodologies confirm trust in several ways, but the nature of ever evolving security breaches violates the concept of trust and break the cloud system integrity. Ensuring trust is the main criteria for the organization when adopting cloud. Following table 8 presented the evaluated articles. Each article is scrutinized against strength and efficiency. The first column in table 9 is represented as the article name where the second column is represented as the proposed approach. Third and fourth column is strength and efficiency. Among the standard QoS criteria for ensuring trust, the authors have highlighted significant criteria for proposing a cloud trust model.

Table 9. *Tabular representation of the cloud trust models*

Article name	Methodology Proposed	Strength	Efficiency
Trust Model for Measuring Security Strength of Cloud Computing Service [122]	A trust model to measures the security strength & compute trust value.	Is calculated by weighted sum.	Evaluation and testing proves the efficiency

Trust Model for Cloud Based on Cloud Characteristics. [2]	A trust model based on the essential cloud characteristics defined by CSA	i) Filtering capability to filter out the negative feedback. ii) Evaluation of trust based on reliability, reputation, credibility	i) Robustness is proven against ii) Experiments are done in a simulator to provide efficiency.
A Cloud Service Trust Evaluation Model Based on Combining Weights and Grey Correlation Analysis [107]	A dynamic trust evaluation model(CSTEM) by combining weight and grey correlation analysis	Experiments of cloud services trust evaluation model (CSTEM) is evaluated in cloud simulator	Robustness and efficiency prove the comprehensiveness.
A Cloud Trust Model in a Security Aware Cloud [109]	'Security Aware Cloud' is proposed to mitigate the social security issues.	Calculation of Internal trust and contracted trust	ROI optimization is done by controlling the quality of service and security
A trust model of cloud computing based on Quality of Service [116]	A trust model based on past credentials and present capabilities of CSP	This model outperform from the conventional FIFO model and other QoS modle	Availability, Turnaround efficiency, integrity, reliability is used to evaluate trust
Trust Model for Optimized Cloud Services [124]	A reputation-based trust model named OPTIMIS to optimize & deal with uncertainty issues of cloud service	Empirical examples and calculation of trust value is strong enough	Prototype tool & experiments with real-life data set evaluate the efficiency
Trust Model to Enhance Security & Interoperability of Cloud Environment [103]	A novel trust model to ensure security in cross-cloud scenario	Ensures identity authentication and behaviour authentication.	Emulation experiments prove the efficiency & safety
Cloudadvisor – A FrameworkTowards Assessing The [86]trustworthiness And Transparency Of Cloud Providers [125]	Cloud Advisor to ensure trustworthiness & transparency	Give assurance to the client or enterprise about choosing the cloud	No
A trust management framework for clouds [126]	A trust management framework based on measurement theory consists of two metrics: trustworthiness and confidence	guideline to the cloud administrator and the cloud customer for making a decision about choosing cloud service, shifting tasks from suspected nodes to trustworthy nodes,	Redundancy, efficiency, and performance are evaluated
A centralized trust model approach for cloud computing [127]	historical feedback helps third party cloud auditor to establish unbiased trust between trustor and the trustee.	Real-time trust value calculation makes the model easy to update.	Effectiveness is calculated based on empirical study.
Cloud Armor: Supporting Reputation-based Trust Management for Cloud Services [112]	Proposed a framework based on reputation which delivers trust as a service (cloudArmor)	Reliability is used to derive the trustworthiness of feedback, which identifies honest cloud	The experimental result shows the capability of detecting any malicious activity in the cloud.
A Trust Evaluation Model for Cloud Computing Using Service Level Agreement [128]	A trust mining model to recognize trust by using Rough set theory and Bayesian inference	This model is compatible with cloud servers and cloud consumers	Accuracy & Performance monitoring is tested by the comparative study
Enhancing Trust Management in Cloud Environment [129]	A multi-faceted trust mechanism to tackle feedback related issues	It filtered out feedback related vulnerabilities and verified suspicious feedback	Performance is tested on a simulated environment , and results show high effectiveness
A Secure and Reputation Based Recommendation Framework for Cloud Services [130]	SRRFCS, a cloud framework to provide cloud trust as a service (TaaS)	Enables the users to efficiently identify and access the cloud services of the trusted CSPs	A real-time setup tests feedback & measures performance, availability, computational complexity, execution time & caching error detection.

CloudAuditor: A Cloud Auditing Framework based on Nested Virtualization [131]	A framework of cloud auditor to examine the behaviour of cloud.	Successful to track suspicious behavior of cloud platform	Performance calculated proves the efficiency
A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security [132]	WAY (Who Are You?), rusted and collaborative agent-based two-tier framework	Ensures security and privacy from CSP's end and client's end.	Performance analysis is given based on the data set.
Design and implementation of a trusted monitoring framework for cloud platforms [133]	VM monitoring framework to provide trust by excluding untrusted domains, by deploying a guest domain for monitoring.	Does not store the previous system state at VM monitoring. Checkpoint is not necessary	Proper experiments are done for performance analysis and efficiency, fault tolerance. Performance is moderate here.
Defining Intercloud Security Framework and Architecture Components for Multi-cloud Data Intensive Applications [134]	Exhibit the continuing development of the Intercloud Security Framework (ICSF), which is a part of Intercloud Architecture Framework	It results in function requirements, Lifecycle of Security Services Management in the cloud.	Discussed security compliances. Trust Bootstrapping Protocol implementation to ensures trust
Collaborative SLA and reputation-based trust management in cloud federations [113]	Collaborative SLA and Reputation-based Trust Management (RTM) solution for federated cloud environment	Test their application's performance and give performance indicators for future service provider selection.	Computation of reliability and performance is given. Reputation value is calculated based on real-life scenario using a fuzzy system
A Reliability-based Trust Management Mechanism for Cloud Services [135]	A trust management framework to filter the reliable user feedback to compute trust	Bridge the trust gap between CSP & users. Reliability calculation familiarity and consistency	Experimental values prove Effectiveness and robustness

3.3.7 Comparative analysis of the state-of-the-art of cloud trust models

In the light of the survey of the contemporary techniques in the above section of cloud trust models, a comprehensive analysis of cloud security principles is presented. Confidentiality, Integrity, Availability, and Privacy are taken as parameters, and the above-stated cloud models are analyzed if they conform to the above security principles or not in table 10. ***Yes*** is marked if a proposed model conforms to a particular parameter, and a ***No*** is marked if the model does not enforce that particular parameter. If a article does not discuss any security principles and does not ensure any of them, ***NA*** (Not applicable**)** is put. The first column is represented as the article name and second is represented as the year of the article. Column 3-6 presented Confidentiality, Integrity, Availability, and Privacy accordingly.

Table 10. Comprehensive analysis of security principles of cloud trust models

Article Name	Year	Confidentiality	Integrity	Availability	Privacy
Shaikh et al. [122]	2015	Yes	Yes	Yes	No
Pawar et al. [2]	2013	Yes	Yes	Yes	No
Wang et al.[107]	2019	Yes	Yes	Yes	No
Sato et al. [109]	2010	Yes	Yes	No	No
Manuel et al. [116]	2015	No	Yes	No	Yes
Pawar et al. [124]	2012	No	Yes	No	No
Li et al. [103]	2009	NA	NA	NA	NA
Almanea et al. [125]	2014	No	Yes	No	No
Ruan et al. [126]	2019	No	No	Yes	Yes
Rizvi et al. [127]	2014	No	No	Yes	No
Talal H Noor et al. [112]	2014	No	No	Yes	Yes
D. Marudhadevi et al. [128]	2015	NA	Yes	NA	NA
Chong et al. [129]	2014	NA	NA	NA	NA
Thangapandiyan et al. [130]	2016	No	No	Yes	No
Zhe Wang et al. [131]	2016	NA	NA	NA	NA
Pal et.al [132]	2011	No	No	Yes	Yes
Zou et al [133]	2013	No	Yes	No	No
Demchenko et al [134]	2017	Yes	Yes	Yes	Yes

Konstantinos et al. [113]	2019	NA	NA	NA	NA
Fan et al [135]	2013	NA	NA	NA	NA

4. Current trends analysis based on the security metrics

Classified frameworks according to the specified journal or conference on the related domain of cloud storage, cloud web service level , and cloud trust level are evaluated based on some crucial security principles viz— confidentiality, Integrity, and Availability in above. Based on the observation in of the total number of article explored over the three-segments it is visible from the following pie chart that the authors are mostly concentrating on conforming confidentiality and integrity. Availability issues is less addressed compared to confidentialty and integrity in Figure 6.

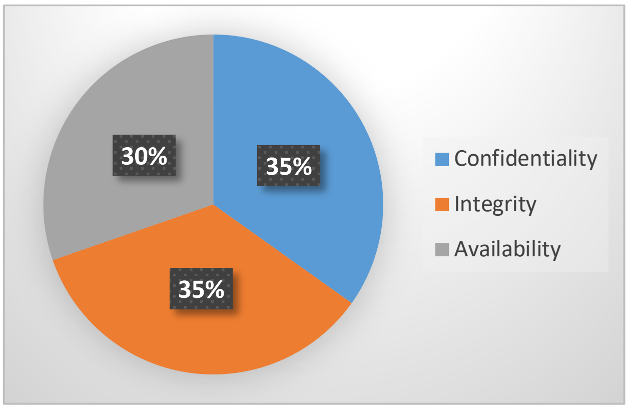

Fig. 6. Evaluation of the recent trends according to the security principles

4.1 Evaluation With the Existing Work

This article scrutinize the current according in the field of cloud storage ,cloud service level issues and trust levelissues. The novelty of this work is to highlight the security breaches based on confidentiality, Integrity and Availability (CIA principle). This article evaluate each of this article whether they ensuring any of the CIA triad or not. A comparative table has been presented in each section to presented this clearly. By analysing the research gap from each section we can produce some future research guideline here.

It is clearly visible from the cloud storage that data is authenticated by the method of cryptography and combination of several data hiding methodologies. But the problem is when the original data is encrypted or it is hidden by any of the data hiding methods it incurs computational overhead and the process is become complex. Apart from this exchaniging of keys between recipient and receiver also leads to security issues. As the cloud storage is concern about data storage spcace, by enveloping the original message into cover file takes extra storage space. By analysing this issues we suggest a data hiding scheme to store the cover secret mapping instead of original information in cloud. As the original message is not stored in cloud storage directly the data integrity, confidentiality is preserved. This mapping must be decrypted by the appropriate receiver by employing keys only. By viewing the cover secret message it is hard to deduce the original message which required keys and cover file. With this context we proposed an article [50] to preserve CIA triad woth privacy and data recoverability-. Our work is experimented with image file. In future this work will be exptended to experiment with different file media in cloud storage.

This article highlight web based cloud services and security issues revolving this area only. Employees within an organization faces several security challenges regarding this area. Authentication problem is a major security issues which os found as a research gap from existing work. If authentication problem arises, it automatically violate data confidentiality and integrity in cloud. An access control policy should be made as a future work to ensure confidentiality , integrity and availability (CIA triad) principals. This acess control policy will check the device before authenticating.

To discuss with cloud trust issues , significant research has been done to ensure trust. Most of the research work is based on recommendation and repuration based model. Ranking methodologies have been employed to rank the cloud service provider (CSP) for analysing suitable choice based on QoS criteria. Different QoS criteria has been evaluated till date to ensure trust. But it is observed no significant research has been there which highlight the security principal. Exisitng attacks does not computed to rank the CSPs. Different deceision making ranking methods has been used based on qualitative criteria, quatitative criteria, fuzzy criteria , crisp criteria and rest. By analysing the existing framework and evaluated each criteria we can suggest security issues should be considered a sone of the significant criteria of QoS. We suggest a decision making method by using artificial intelligence highlighting security issues with other significant QoS criteria as well. Artificla intelligence will help to take a decision instead of any third party which helps to increase trust.

5. Conclusion

This article introduces a detailed survey of the recent threats and challenges that exist in the cloud storage layer, cloud service layer , and cloud trust layer. The individual field is explained with their mitigation framework proposed to prevent security challenges and threats. Each segment is composed of a well-defined definition, classification. Apart from discussing the framework proposed, a comprehensive analysis table is presented where it shows that the proposed framework is conformed to the confidentiality, Integrity, Availability, Data Recovery principle. It is observable from the survey that the framework suffers from several weaknesses that can be enhanced as future work. In maximum cases, the proposed framework incurs an extra computational cost and does not have any accuracy or robustness calculation. Some technique does not ensure CIA principle , and some have not work on security parameter. For storage security, authors, in maximum cases, omit the data recoverability issues. Less research work is found which conform to security over in-transit data.

For over a decade cloud has been considered a standard IT platform and a robust data-centric architecture where the cloud resources are scalable, efficient enough to meet the customer's needs and help in the growth of an enterprise. However, with the rise of real-time computing demands, technology giants forced technology to shift from centralized cloud frameworks to a distributed architecture. The exponential growth, cost reduction of IoT devices have given a new horizon to edge computing by extending cloud technologies. In cloud computing, IoT devices generate the data and send it to the cloud server for processing. It incurs network latency, faces several security attacks. However, in edge computing, an edge resides in the middle of IoT devices and cloud servers to reduce network latency, increase accuracy. Cloud is replaced with another decentralized AI-based service named blockchain, which supports the cryptocurrency currently. Each file in decentralized storage is stored, encrypted and customers can be assured that the data will be secured as it is decentralized in nature and blockchain technology is used, which is difficult for the attacker to break the hash.

References

1. Ab Rahman, N.H., Choo, K.-K.R.: A survey of information security incident handling in the cloud. Computers & Security. 49, 45–69 (2015). https://doi.org/10.1016/j.cose.2014.11.006.
2. Pawar, P.S., Rajarajan, M., Dimitrakos, T., Zisman, A.: Trust Model for Cloud Based on Cloud Characteristics. In: Fernández-Gago, C., Martinelli, F., Pearson, S., and Agudo, I. (eds.) Trust Management VII. pp. 239–246. Springer Berlin Heidelberg, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38323-6_18.
3. Sun, P.: Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications. 160, 102642 (2020). https://doi.org/10.1016/j.jnca.2020.102642.
4. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 34, 1–11 (2011). https://doi.org/10.1016/j.jnca.2010.07.006.
5. Kaaniche, N., Laurent, M.: Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications. 111, 120–141 (2017). https://doi.org/10.1016/j.comcom.2017.07.006.
6. Pearson, S., Benameur, A.: Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science. pp. 693–702. IEEE, Indianapolis, IN, USA (2010). https://doi.org/10.1109/CloudCom.2010.66.
7. Singh, A., Chatterjee, K.: Cloud security issues and challenges. J. Netw. Comput. Appl. 79, 88–115 (2017). https://doi.org/10.1016/j.jnca.2016.11.027.
8. Hatcher, W.G., Yu, W., Nguyen, J.H., Wei, S., Chen, Z.: A cloud/edge computing streaming system for network traffic monitoring and threat detection. IJSN. 13, 169 (2018). https://doi.org/10.1504/IJSN.2018.10014317.
9. Khan, M.A.: A survey of security issues for cloud computing. Journal of Network and Computer Applications. 71, 11–29 (2016). https://doi.org/10.1016/j.jnca.2016.05.010.
10. Cusack, B., Ghazizadeh, E.: Analysing Trust Issues in Cloud Identity Environments. 16 (2016).
11. Writing a Systematic Literature Review – JEPS Bulletin, https://blog.efpsa.org/2018/01/03/writing-a-systematic-literature-review/, last accessed 2020/07/03.
12. Chiregi, M., Jafari Navimipour, N.: Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms. Journal of Electrical Systems and Information Technology. 5, 608–622 (2018). https://doi.org/10.1016/j.jesit.2017.09.001.
13. Hussain, W., Hussain, F.K., Hussain, O.K., Damiani, E., Chang, E.: Formulating and managing viable SLAs in cloud computing from a small to medium service provider's viewpoint: A state-of-the-art review. Information Systems. 71, 240–259 (2017). https://doi.org/10.1016/j.is.2017.08.007.
14. Novais, L., Maqueira, J.M., Ortiz-Bas, Á.: A systematic literature review of cloud computing use in supply chain integration. Computers & Industrial Engineering. 129, 296–314 (2019). https://doi.org/10.1016/j.cie.2019.01.056.
15. Milani, B.A., Navimipour, N.J.: A Systematic Literature Review of the Data Replication Techniques in the Cloud Environments. Big Data Research. 10, 1–7 (2017). https://doi.org/10.1016/j.bdr.2017.06.003.
16. Ibrahim, F., Hemayed, E.: Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. Comput. Secur. (2019). https://doi.org/10.1016/J.COSE.2018.12.014.
17. Souri, A., Navimipour, N.J., Rahmani, A.M.: Formal verification approaches and standards in the cloud computing: A comprehensive and systematic review. Computer Standards & Interfaces. 58, 1–22 (2018). https://doi.org/10.1016/j.csi.2017.11.007.
18. Kumar, R., Goyal, R.: On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review. 33, 1–48 (2019). https://doi.org/10.1016/j.cosrev.2019.05.002.
19. Banijamali, A., Pakanen, O.-P., Kuvaja, P., Oivo, M.: Software architectures of the convergence of cloud computing and the Internet of Things: A systematic literature review. Information and Software Technology. 122, 106271 (2020). https://doi.org/10.1016/j.infsof.2020.106271.
20. Rajan, R.A.P.: Evolution of Cloud Storage as Cloud Computing Infrastructure Service. IOSRJCE. 1, 38–45 (2012). https://doi.org/10.9790/0661-0113845.
21. Liu, K., Dong, L.-J.: Research on Cloud Data Storage Technology and Its Architecture Implementation. Procedia Engineering. 29, (2012).
22. Kulkarni, G., Waghmare, R., Palwe, R., Waykule, V., Bankar, H., Koli, K.: Cloud storage architecture. In: 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA). pp. 76–81. IEEE, Denpasar-Bali, Indonesia (2012). https://doi.org/10.1109/TSSA.2012.6366026.
23. Vurukonda, N., Rao, B.T.: A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science. 92, (2016).
24. Anatomy of a cloud storage infrastructure, https://developer.ibm.com/depmodels/cloud/articles/cl-cloudstorage/, last accessed 2020/07/03.
25. Neelima, M.L.: A STUDY ON CLOUD STORAGE. IJCSMC. Vol. 3, pg.966 – 971 (2014).
26. Cloud Data Management Interface (CDMI) | SNIA, https://www.snia.org/cdmi, last accessed 2020/07/03.
27. Puttaswamy, K.P.N., Kruegel, C., Zhao, B.Y.: Silverline: toward data confidentiality in storage-intensive cloud applications. In: Proceedings of the 2nd ACM Symposium on Cloud Computing - SOCC '11. pp. 1–13. ACM Press, Cascais, Portugal (2011). https://doi.org/10.1145/2038916.2038926.
28. M., S., S., S., Thomas, A.: Generic cost optimized and secured sensitive attribute storage model for template based text document on cloud. Computer Communications. 150, 569–580 (2020). https://doi.org/10.1016/j.comcom.2019.11.029.
29. DeCusatis, C., Liengtiraphan, P., Sager, A., Pinelli, M.: Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. In: 2016 IEEE International Conference on Smart Cloud (SmartCloud). pp. 5–10. IEEE, New York, NY, USA (2016). https://doi.org/10.1109/SmartCloud.2016.22.
30. Mary, B.F., Amalarethinam, D.I.G.: Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography. In: 2017 World Congress on Computing and Communication Technologies (WCCCT). pp. 181–184 (2017). https://doi.org/10.1109/WCCCT.2016.52.
31. Shibli, M.A., Masood, R., Habiba, U., Kanwal, A., Ghazi, Y., Mumtaz, R.: Access Control As a Service in Cloud: Challenges, Impact and Strategies. In: Mahmood, Z. (ed.) Continued Rise of the Cloud: Advances and Trends in Cloud Computing. pp. 55–99. Springer, London (2014). https://doi.org/10.1007/978-1-4471-6452-4_3.
32. Padhy, R.P.: Cloud Computing: Security Issues and Research Challenges. International Journal of Computer Science and Information Technology. 1, 11 (2011).

33. Lin, Y.: Public Integrity Auditing for Cloud Storage based on Consortium Blockchain | IEEE Communications Society, https://www.comsoc.org/publications/tcn/2019-nov/public-integrity-auditing-cloud-storage-based-consortium-blockchain, last accessed 2020/07/04.
34. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou: Ensuring data storage security in Cloud Computing. In: 2009 17th International Workshop on Quality of Service. pp. 1–9 (2009). https://doi.org/10.1109/IWQoS.2009.5201385.
35. Gantz, J.: The Digital Universe Decade Are You Ready?, https://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf.
36. Hou, H., Yu, J., Hao, R.: Cloud storage auditing with deduplication supporting different security levels according to data popularity. Journal of Network and Computer Applications. 134, 26–39 (2019). https://doi.org/10.1016/j.jnca.2019.02.015.
37. Kaur, R., Chana, I., Bhattacharya, J.: Data deduplication techniques for efficient cloud storage management: a systematic review. J Supercomput. 74, 2035–2085 (2018). https://doi.org/10.1007/s11227-017-2210-8.
38. (PDF) [IJCST-V5I4P4]: Purnima,Deepak Kumar Verma | IJCST Eighth Sense Research Group - Academia.edu, https://www.academia.edu/33913804/_IJCST-V5I4P4_Purnima_Deepak_Kumar_Verma, last accessed 2020/07/03.
39. Jiang, W., Zhao, Z., Laat, C. de: An Autonomous Security Storage Solution for Data-Intensive Cooperative Cloud Computing. In: 2013 IEEE 9th International Conference on e-Science. pp. 369–372 (2013). https://doi.org/10.1109/eScience.2013.31.
40. Govinda Raju, K., Nanna Babu, P., Phani Sridhar, A., Srinivasulu, T.: QABA: A privacy model to reduce adversary attacks for cloud storage. Materials Today: Proceedings. (2020). https://doi.org/10.1016/j.matpr.2020.11.483.
41. Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: towards a cloud definition. SIGCOMM Comput. Commun. Rev. 39, 50–55 (2008). https://doi.org/10.1145/1496091.1496100.
42. Tari, Z.: Security and Privacy in Cloud Computing. IEEE Cloud Comput. 1, 54–57 (2014). https://doi.org/10.1109/MCC.2014.20.
43. Tang, Y., Lee, P.P.C., Lui, J.C.S., Perlman, R.: FADE: Secure Overlay Cloud Storage with File Assured Deletion. In: Jajodia, S. and Zhou, J. (eds.) Security and Privacy in Communication Networks. pp. 380–397. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-16161-2_22.
44. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A.V.: Security and privacy for storage and computation in cloud computing. Information Sciences. 258, 371–386 (2014). https://doi.org/10.1016/j.ins.2013.04.028.
45. Yan, Y.X., Wu, L., Xu, W.Y., Wang, H., Liu, Z.M.: Integrity Audit of Shared Cloud Data with Identity Tracking, https://www.hindawi.com/journals/scn/2019/1354346/, last accessed 2020/07/03. https://doi.org/10.1155/2019/1354346.
46. Nandini, J.: SECURE MULTI-OWNER DATA STORAGE WITH ENHANCED TPA AUDITING SCHEME IN CLOUD COMPUTING. International Journal of Advances In Computer Science and Cloud Computing. Volume-2, (2014).
47. Wang, W., Ren, L., Chen, L., Ding, Y.: Intrusion detection and security calculation in industrial cloud storage based on an improved dynamic immune algorithm. Information Sciences. 501, 543–557 (2019). https://doi.org/10.1016/j.ins.2018.06.072.
48. Shen, W., Qin, J., Yu, J., Hao, R., Hu, J., Ma, J.: Data Integrity Auditing without Private Key Storage for Secure Cloud Storage. IEEE Transactions on Cloud Computing. 1–1 (2019). https://doi.org/10.1109/TCC.2019.2921553.
49. Yang, J., Zhu, H., Liu, T.: Secure and economical multi-cloud storage policy with NSGA-II-C. Appl. Soft Comput. (2019). https://doi.org/10.1016/J.ASOC.2019.105649.
50. Mandal, S., Khan, D.A.: A Dynamic Programming Approach to Secure User Image Data in Cloud Based ERP Systems. In: 2019 Fifth International Conference on Image Information Processing (ICIIP). pp. 91–96 (2019). https://doi.org/10.1109/ICIIP47207.2019.8985974.
51. Liu, Q., Wang, G., Wu, J.: Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inf. Sci. (2014). https://doi.org/10.1016/j.ins.2012.09.034.
52. Yesilyurt, M., Yalman, Y.: New approach for ensuring cloud computing security: using data hiding methods. Sādhanā. 41, 1289–1298 (2016). https://doi.org/10.1007/s12046-016-0558-8.
53. Wang, R.: Research on Data Security Technology Based on Cloud Storage. (2017). https://doi.org/10.1016/j.proeng.2017.01.286.
54. Mall, S., Saroj, S.K.: A New Security Framework for Cloud Data. Procedia Computer Science. 143, 765–775 (2018). https://doi.org/10.1016/j.procs.2018.10.397.
55. Prabhu kavin, B., Ganapathy, S.: A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks. 151, 181–190 (2019). https://doi.org/10.1016/j.comnet.2019.01.032.
56. Sun, A., Gao, G., Ji, T., Tu, X.: One Quantifiable Security Evaluation Model for Cloud Computing Platform. In: 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD). pp. 197–201 (2018). https://doi.org/10.1109/CBD.2018.00043.
57. Arthur Sandor, V.K., Lin, Y., Li, X., Lin, F., Zhang, S.: Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage. Journal of Network and Computer Applications. 129, 25–36 (2019). https://doi.org/10.1016/j.jnca.2019.01.003.
58. Zhang, J., Yuan, D., Cui, L., Zhou, B.B.: A highly efficient algorithm towards optimal data storage and regeneration cost in multiple clouds. Future Generation Computer Systems. 99, 459–472 (2019). https://doi.org/10.1016/j.future.2019.04.002.
59. Hawedi, M., Talhi, C., Boucheneb, H.: Security as a Service for Public Cloud Tenants(SaaS). Procedia Computer Science. 130, 1025–1030 (2018). https://doi.org/10.1016/j.procs.2018.04.143.
60. Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M.: A survey on security issues and solutions at different layers of Cloud computing. J Supercomput. 63, 561–592 (2013). https://doi.org/10.1007/s11227-012-0831-5.
61. What is cloud services? - Definition from WhatIs.com, https://searchitchannel.techtarget.com/definition/cloud-services, last accessed 2020/07/03.
62. Applications As a Service, https://apprenda.com/library/software-on-demand/applications-as-a-service/, last accessed 2020/07/03.
63. Elsayed, M., Zulkernine, M.: Offering security diagnosis as a service for cloud SaaS applications. Journal of Information Security and Applications. 44, 32–48 (2019). https://doi.org/10.1016/j.jisa.2018.11.006.
64. Dacosta, I., Chakradeo, S., Ahamad, M., Traynor, P.: One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. ACM Trans. Internet Technol. 12, 1–24 (2012). https://doi.org/10.1145/2220352.2220353.
65. Ping-Chen, X.: SQL injection attack and guard technical research. Procedia Engineering. 15, 4131–4135 (2011). https://doi.org/10.1016/j.proeng.2011.08.775.
66. Prapty, R.T., Md, S.A., Hossain, S., Narman, H.S.: Preventing Session Hijacking using Encrypted One-Time-Cookies. In: 2020 Wireless Telecommunications Symposium (WTS). pp. 1–6 (2020). https://doi.org/10.1109/WTS48268.2020.9198717.
67. Kwon, H.: Detecting Backdoor Attacks via Class Difference in Deep Neural Networks. IEEE Access. 8, 191049–191056 (2020). https://doi.org/10.1109/ACCESS.2020.3032411.
68. Dai, J., Chen, C., Li, Y.: A Backdoor Attack Against LSTM-Based Text Classification Systems. IEEE Access. 7, 138872–138878 (2019). https://doi.org/10.1109/ACCESS.2019.2941376.
69. Halabi, T., Bellaiche, M.: Towards quantification and evaluation of security of Cloud Service Providers. Journal of Information Security and Applications. 33, 55–65 (2017). https://doi.org/10.1016/j.jisa.2017.01.007.
70. Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S.: A Survey on Security Issues in Cloud Computing. arXiv:1109.5388 [cs]. (2013).
71. Shubh, T., Sharma, S.: Man-In-The-Middle-Attack Prevention Using HTTPS and SSL. 11 (2016).
72. Kumar, S.S.: Analysis on Man in the Middle Attack on SSL Pushpendra Kumar Pateriya.
73. Chen, J., Luo, X., Guo, Y., Zhang, Y., Gong, D.: A Survey on Breaking Technique of Text-Based CAPTCHA. Security and Communication Networks. (2017). https://doi.org/10.1155/2017/6898617.
74. Bajtoš, T., Gajdoš, A., Kleinová, L., Lučivjanská, K., Sokol, P.: Network Intrusion Detection with Threat Agent Profiling. Security and Communication Networks. 2018, 1–17 (2018). https://doi.org/10.1155/2018/3614093.
75. Gonzalez, J.J., Sarriegi, J.M., Gurrutxaga, A.: A Framework for Conceptualizing Social Engineering Attacks. In: Lopez, J. (ed.) Critical Information Infrastructures Security. pp. 79–90. Springer, Berlin, Heidelberg (2006). https://doi.org/10.1007/11962977_7.
76. Ahmad, S., Ehsan, B.: The Cloud Computing Security Secure User Authentication Technique(Multi Level Authentication). 4, 6 (2013).

77. Wu, Z., Tian, L., Li, P., Wu, T., Jiang, M., Wu, C.: Generating stable biometric keys for flexible cloud computing authentication using finger vein. Information Sciences. 433–434, 431–447 (2018). https://doi.org/10.1016/j.ins.2016.12.048.
78. Goyal, V., Kumar, V., Singh, M., Abraham, A., Sanyal, S.: CompChall: addressing password guessing attacks. In: International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II. pp. 739-744 Vol. 1 (2005). https://doi.org/10.1109/ITCC.2005.107.
79. Babkin, S., Epishkina, A.: One-Time Passwords: Resistance to Masquerade Attack. Procedia Computer Science. 145, 199–203 (2018). https://doi.org/10.1016/j.procs.2018.11.040.
80. Jurcut, A.D., Coffey, T., Dojen, R.: On the Prevention and Detection of Replay Attacks Using a Logic-Based Verification Tool. In: Kwiecień, A., Gaj, P., and Stera, P. (eds.) Computer Networks. pp. 128–137. Springer International Publishing, Cham (2014). https://doi.org/10.1007/978-3-319-07941-7_13.
81. Tapiador, J.E., Clark, J.A.: Masquerade mimicry attack detection: A randomised approach. Computers & Security. 30, 297–310 (2011). https://doi.org/10.1016/j.cose.2011.05.004.
82. Duncan, A.J., Creese, S., Goldsmith, M.: Insider Attacks in Cloud Computing. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. pp. 857–862 (2012). https://doi.org/10.1109/TrustCom.2012.188.
83. Bekerman, D., Shapira, B., Rokach, L., Bar, A.: Unknown malware detection using network traffic classification. In: 2015 IEEE Conference on Communications and Network Security (CNS). pp. 134–142. IEEE, Florence, Italy (2015). https://doi.org/10.1109/CNS.2015.7346821.
84. Varshney, G., Misra, M., Atrey, P.K.: A phish detector using lightweight search features. Computers & Security. 62, 213–228 (2016). https://doi.org/10.1016/j.cose.2016.08.003.
85. Lashkari, A.H., Farmand, S., Zakaria, D.O.B., Saleh, D.R.: Shoulder Surfing attack in graphical password authentication. arXiv:0912.0951 [cs]. (2009).
86. Jouini, M., Rabai, L.B.A.: Security Problems in Cloud Computing Environments: A Deep Analysis and a Secure Framework. Presented at the (2017). https://doi.org/10.4018/978-1-5225-2449-6.ch004.
87. Laborde, R., Barrère, F., Benzekri, A.: Toward Authorization as a Service: A Study of the XACML Standard. Presented at the 16th Communications and Networking Symposium (CNS 2013) in 2013 Spring Simulation Multi-Conference (2013).
88. Ukil, A., Jana, D., De Sarkar, A.: A Security Framework in Cloud Computing Infrastructure. IJNSA. 5, 11–24 (2013). https://doi.org/10.5121/ijnsa.2013.5502.
89. Hussain, S.A., Fatima, M., Saeed, A., Raza, I., Shahzad, R.K.: Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics. 13, 57–65 (2017). https://doi.org/10.1016/j.aci.2016.03.001.
90. Ramachandran, M., Chang, V.: Towards Performance Evaluation of Cloud Service Providers for Cloud Data Security. International Journal of Information Management. 36, 618–625 (2016). https://doi.org/Ramachandran, Muthu and Chang, Victor (2016) Towards Performance Evaluation of Cloud Service Providers for Cloud Data Security. International Journal of Information Management, 36 (4), 618-625. (doi:10.1016/j.ijinfomgt.2016.03.005 <http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.005>).
91. Potey, M.M., Dhote, C.A., Sharma, D.H.: Homomorphic Encryption for Security of Cloud Data. Procedia Computer Science. 79, 175–181 (2016). https://doi.org/10.1016/j.procs.2016.03.023.
92. Casola, V., De Benedictis, A., Rak, M., Villano, U.: Security-by-design in multi-cloud applications: An optimization approach. Information Sciences. 454–455, 344–362 (2018). https://doi.org/10.1016/j.ins.2018.04.081.
93. Hudic, A., Smith, P., Weippl, E.R.: Security assurance assessment methodology for hybrid clouds. Computers & Security. 70, 723–743 (2017). https://doi.org/10.1016/j.cose.2017.03.009.
94. Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., Xiang, Y.: Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing. IEEE Transactions on Dependable and Secure Computing. 16, 996–1010 (2019). https://doi.org/10.1109/TDSC.2017.2725953.
95. Zhou, L., Li, X., Yeh, K.-H., Su, C., Chiu, W.: Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems. 91, 244–251 (2019). https://doi.org/10.1016/j.future.2018.08.038.
96. Kumar, P., Singhal, A., Saini, R., Roy, P.P., Dogra, D.P.: A pervasive electroencephalography-based person authentication system for cloud environment. Displays. 55, 64–70 (2018). https://doi.org/10.1016/j.displa.2018.09.006.
97. Deshmukh, P.: Design of cloud security in the EHR for Indian healthcare services. Journal of King Saud University - Computer and Information Sciences. 29, 281–287 (2017). https://doi.org/10.1016/j.jksuci.2016.01.002.
98. Tao, M., Zuo, J., Liu, Z., Castiglione, A., Palmieri, F.: Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Generation Computer Systems. 78, 1040–1051 (2018). https://doi.org/10.1016/j.future.2016.11.011.
99. Arpaci, I., Kilicer, K., Bardakci, S.: Effects of security and privacy concerns on educational use of cloud services. Computers in Human Behavior. 45, 93–98 (2015). https://doi.org/10.1016/j.chb.2014.11.075.
100. Yang, Y., Liu, R., Chen, Y., Li, T., Tang, Y.: Normal Cloud Model-Based Algorithm for Multi-Attribute Trusted Cloud Service Selection. IEEE Access. 6, 37644–37652 (2018). https://doi.org/10.1109/ACCESS.2018.2850050.
101. Ritu, Randhawa, S., Jain, S.: Trust Models in Cloud Computing: A Review. IJWMT. 7, 14–27 (2017). https://doi.org/10.5815/ijwmt.2017.04.02.
102. Emeakaroha, V.C., Fatema, K., Werff, L. v d, Healy, P., Lynn, T., Morrison, J.P.: A Trust Label System for Communicating Trust in Cloud Services. IEEE Transactions on Services Computing. 10, 689–700 (2017). https://doi.org/10.1109/TSC.2016.2553036.
103. Li, W., Ping, L.: Trust Model to Enhance Security and Interoperability of Cloud Environment. In: Jaatun, M.G., Zhao, G., and Rong, C. (eds.) Cloud Computing. pp. 69–79. Springer, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10665-1_7.
104. Dou, Y., Chan, H.C.B., Au, M.H.: A Distributed Trust Evaluation Protocol with Privacy Protection for Intercloud. IEEE Transactions on Parallel and Distributed Systems. 30, 1208–1221 (2019). https://doi.org/10.1109/TPDS.2018.2883080.
105. Kesarwani, A., Khilar, P.M.: Development of trust based access control models using fuzzy logic in cloud computing. Journal of King Saud University - Computer and Information Sciences. (2019). https://doi.org/10.1016/j.jksuci.2019.11.001.
106. Govindaraj, P., Jaisankar, N., School of Computer Science and Engineering, VIT University, Vellore, India: A Review on Various Trust Models in Cloud Environment. JESTR. 10, 213–219 (2017). https://doi.org/10.25103/jestr.102.24.
107. Wang, Y., Wen, J., Wang, X., Tao, B., Zhou, W.: A Cloud Service Trust Evaluation Model Based on Combining Weights and Gray Correlation Analysis. Security and Communication Networks. 2019, 1–11 (2019). https://doi.org/10.1155/2019/2437062.
108. Demigha, O., Larguet, R.: Hardware-based solutions for trusted cloud computing. Computers & Security. 103, 102117 (2021). https://doi.org/10.1016/j.cose.2020.102117.
109. Sato, H., Kanai, A., Tanimoto, S.: A Cloud Trust Model in a Security Aware Cloud. In: 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet. pp. 121–124 (2010). https://doi.org/10.1109/SAINT.2010.13.
110. Mujawar, T.N., Bhajantri, L.B.: Behavior and feedback based trust computation in cloud environment. Journal of King Saud University - Computer and Information Sciences. (2020). https://doi.org/10.1016/j.jksuci.2020.12.003.
111. Liang, J., Zhang, M., Leung, V.C.M.: A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud. IEEE Internet of Things Journal. 7, 5481–5490 (2020). https://doi.org/10.1109/JIOT.2020.2981005.
112. Noor, T.H., Sheng, Q.Z., Yao, L., Dustdar, S., Ngu, A.H.H.: CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services. IEEE Trans. Parallel Distrib. Syst. 27, 367–380 (2016). https://doi.org/10.1109/TPDS.2015.2408613.
113. Papadakis-Vlachopapadopoulos, K., González, R.S., Dimolitsas, I., Dechouniotis, D., Ferrer, A.J., Papavassiliou, S.: Collaborative SLA and reputation-based trust management in cloud federations. Future Generation Computer Systems. 100, 498–512 (2019). https://doi.org/10.1016/j.future.2019.05.030.
114. Huang, C., Chen, W., Yuan, L., Ding, Y., Jian, S., Tan, Y., Chen, H., Chen, D.: Toward security as a service: A trusted cloud service architecture with policy customization. Journal of Parallel and Distributed Computing. 149, 76–88 (2021). https://doi.org/10.1016/j.jpdc.2020.11.002.
115. Grandison, T., Sloman, M.: A survey of trust in internet applications. IEEE Commun. Surv. Tutorials. 3, 2–16 (2000). https://doi.org/10.1109/COMST.2000.5340804.

116. Manuel, P.: A trust model of cloud computing based on Quality of Service. Ann Oper Res. 233, 281–292 (2015). https://doi.org/10.1007/s10479-013-1380-x.
117. Dey, S., Sen, S.K.: Trust Evaluation Model in Cloud Using Reputation, Recommendation and QOS Based Approach. In: 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE). pp. 1–5 (2018). https://doi.org/10.1109/RICE.2018.8509061.
118. Rathi, S.R., Kolekar, V.K.: Trust Model for Computing Security of Cloud. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). pp. 1–5 (2018). https://doi.org/10.1109/ICCUBEA.2018.8697881.
119. Pandey, V., Goswami, M.G.: Various challenges and Trust issues in cloud computing for improvement the quality and services. 6.
120. Odun-Ayo, I., Idoko, B.E.: Cloud Trust Management – Issues and Developments. 6 (2018).
121. Bezzi, M., Kaluvuri, S.P., Sabetta, A.: Ensuring trust in service consumption through security certification. In: Proceedings of the International Workshop on Quality Assurance for Service-Based Applications. pp. 40–43. Association for Computing Machinery, Lugano, Switzerland (2011). https://doi.org/10.1145/2031746.2031758.
122. A.r, S.R.: Trust Model for Measuring Security Strength of a Cloud Computing Service. -. (2015).
123. Nissenbaum, H.: Can Trust be Secured Online? A theoretical perspective. Presented at the (1999).
124. Pawar, P.S., Rajarajan, M., Nair, S.K., Zisman, A.: Trust Model for Optimized Cloud Services. In: Dimitrakos, T., Moona, R., Patel, D., and McKnight, D.H. (eds.) Trust Management VI. pp. 97–112. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29852-3_7.
125. Almanea, M.I.M.: Cloud Advisor - A Framework towards Assessing the Trustworthiness and Transparency of Cloud Providers. In: Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. pp. 1018–1019. IEEE Computer Society, USA (2014). https://doi.org/10.1109/UCC.2014.168.
126. Ruan, Y., Durresi, A.: A trust management framework for clouds. Computer Communications. 144, 124–131 (2019). https://doi.org/10.1016/j.comcom.2019.05.018.
127. Rizvi, S., Ryoo, J., Liu, Y., Zazworsky, D., Cappeta, A.: A centralized trust model approach for cloud computing. In: 2014 23rd Wireless and Optical Communication Conference (WOCC). pp. 1–6 (2014). https://doi.org/10.1109/WOCC.2014.6839923.
128. Marudhadevi, D., Dhatchayani, V.N., Sriram, V.S.S.: A Trust Evaluation Model for Cloud Computing Using Service Level Agreement. Comput. J. (2015). https://doi.org/10.1093/comjnl/bxu129.
129. Chong, S.-K., Abawajy, J., Ahmad, M., Hamid, I.R.A.: Enhancing Trust Management in Cloud Environment. Procedia - Social and Behavioral Sciences. 129, 314–321 (2014). https://doi.org/10.1016/j.sbspro.2014.03.682.
130. Thangapandiyan, M., Anand, P.M.R.: A secure and reputation based recommendation framework for cloud services. In: 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). pp. 1–4 (2016). https://doi.org/10.1109/ICCIC.2016.7919611.
131. Wang, Z., Zeng, J., Lv, T., Shi, B., Li, B.: CloudAuditor: A Cloud Auditing Framework Based on Nested Virtualization. In: 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). pp. 50–53 (2016). https://doi.org/10.1109/CSCloud.2016.40.
132. Pal, S., Khatua, S., Chaki, N., Sanyal, S.: A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security. 12.
133. Zou, D., Zhang, W., Qiang, W., Xiang, G., Yang, L.T., Jin, H., Hu, K.: Design and implementation of a trusted monitoring framework for cloud platforms. Future Generation Computer Systems. 29, 2092–2102 (2013). https://doi.org/10.1016/j.future.2012.12.020.
134. Demchenko, Y., Turkmen, F., Slawik, M., Laat, C. de: Defining Intercloud Security Framework and Architecture Components for Multi-cloud Data Intensive Applications. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). pp. 945–952. IEEE, Madrid (2017). https://doi.org/10.1109/CCGRID.2017.144.
135. Fan, W., Perros, H.: A Reliability-Based Trust Management Mechanism for Cloud Services. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. pp. 1581–1586 (2013). https://doi.org/10.1109/TrustCom.2013.194.