Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.026690
Article

Tech Science Press

Towards Developing Privacy-Preserved Data Security Approach (PP-DSA) in Cloud Computing Environment

S. Stewart Kirubakaran[1,*], V. P. Arunachalam[1], S. Karthik[1] and S. Kannan[2]

[1]Department of Computer Science & Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India
[2]School of Computing Science and Engineering, Vellore Institute of Technology, Bhopal, Madhya Pradhesh, India
*Corresponding Author: S. Stewart Kirubakaran. Email: stewartkirubakaran@gmail.com

Received: 01 January 2022; Accepted: 09 March 2022

Abstract: In the present scenario of rapid growth in cloud computing models, several companies and users started to share their data on cloud servers. However, when the model is not completely trusted, the data owners face several security-related problems, such as user privacy breaches, data disclosure, data corruption, and so on, during the process of data outsourcing. For addressing and handling the security-related issues on Cloud, several models were proposed. With that concern, this paper develops a Privacy-Preserved Data Security Approach (PP-DSA) to provide the data security and data integrity for the outsourcing data in Cloud Environment. Privacy preservation is ensured in this work with the Efficient Authentication Technique (EAT) using the Group Signature method that is applied with Third-Party Auditor (TPA). The role of the auditor is to secure the data and guarantee shared data integrity. Additionally, the Cloud Service Provider (CSP) and Data User (DU) can also be the attackers that are to be handled with the EAT. Here, the major objective of the work is to enhance cloud security and thereby, increase Quality of Service (QoS). The results are evaluated based on the model effectiveness, security, and reliability and show that the proposed model provides better results than existing works.

Keywords: Third-party auditor (TPA); efficient auditing technique (EAT); cloud service provider (CSP); data user (DU); data security; privacy-preserving; cloud computing; cloud security

1 Introduction

Cloud models and services are becoming very important in this era for modern and digital communications. Moreover, the cloud model provides infrastructure and software problems [1,2]. Some of the cloud services are, Amazon's simple storage service, Cloud Sae, etc., which uses the customer identity, private data, and the customer location. Since, the cloud models are handling several data privacy and security problems, which has become the greatest confrontation in recent cloud services. The customers or the cloud users, who store their private data like banking details, health data, and so on, have their primary right to data security. There are some cryptographic devices and models like unknown user authentication models, signature schema, and secure protocols. User authentication avoids illegal people from accessing critical information. For example, User A has just related information and cannot get User B's sensitive information. Cybercriminals can get access to a system and they can steal information if user authentication is not secure. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) offer a secure protocol that enables two networked peers to safely interact. SSL is most commonly used to send personal information from a web browser to a web server. TLS encodes data sent through the Internet so that unauthorized people and hackers cannot read it, which is especially beneficial for private and sensitive information such as passwords, credit card numbers, and personal messages. The CSPs are required to be controlled using the authentication process for providing authorized access to the users. Based on that, the malicious users are revoked with their identities.

The cloud resources are used by users based on their requirements with efficient dynamic reliability and service integration process. For example, in processing medical data, the user's private data are to be maintained and processed in a secure model and to be accessible to the authorized health care practitioners [3]. In the existing models in secure cloud data sharing, varied encryption and key distribution models are developed, but still there exists some overhead and computational complexities [4]. Encryption is the most common way of changing plain text information (plaintext) into something that seems arbitrary and unimportant (ciphertext). Decryption is the method involved with changing over ciphertext to plaintext. Symmetric encryption is utilized to scramble a lot of information.

Cloud Computing is considered as the virtualization of the available data services or data center, which provides a multi-purpose model, supports services to multiple clients [5]. Cloud computing is the source for numerous services, such as data storage, servers, databases, networking, and software, over the Internet. The ability to save files to a distant database and retrieve them on demand is enabled by cloud storage. The main benefits of cloud computing are its dependability, pay-per-use pricing, and ease of access. Furthermore, security, recurring costs, and less control over flexibility and infrastructure are considered as disadvantages of cloud computing. In the cloud, the services are provided based on the user requirements [6]. Additionally, the cloud model stores significant data and provides effective user service with a reliable cloud service model [7]. With the effectiveness of new technologies, in addition to the existing services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), new cloud models like Supercomputing as a Service (SCaaS) and High-Performance Computing as a Service (HPCaaS), users attach to and use cloud-based programs over the Internet with the software as a service (SaaS). Email, calendaring, and office tools are some other common examples (from Microsoft Office 365). A cloud service provider offers a complete software system solution that you may pay for on a "pay-as-you-go" basis. Infrastructure as a service (IaaS) stands for a "pay-as-you-go" cloud computing service that delivers on-demand compute, storage, and networking capabilities. IaaS is one among the four cloud service types, along with software as a service (SaaS), platform as a service (PaaS), and serverless. PaaS is a comprehensive cloud development and deployment environment that includes tools for the creation of everything from a simple cloud-based app to a classy cloud-based enterprise system.

In general, the typical common elements of the cloud data model contain Data Owner (DO), Data User (DU), and the Cloud Service Provider (CSP), presented in Fig. 1. The data owner outsources their data onto the cloud by using its storage. Further, the DO entails the cloud that can provide more services like data computation, data search, and sharing. The data user is the category that utilizes the cloud data and performs operations, such as data retrieval, data gathering, data computation, and access. Moreover, the CSP has enormous storage and computational space, and the CSP is responsible for allocating services for data consumers when there is a demand in the cloud environment. In some cases, the data owners may take the responsibility of providing services, as CSP.

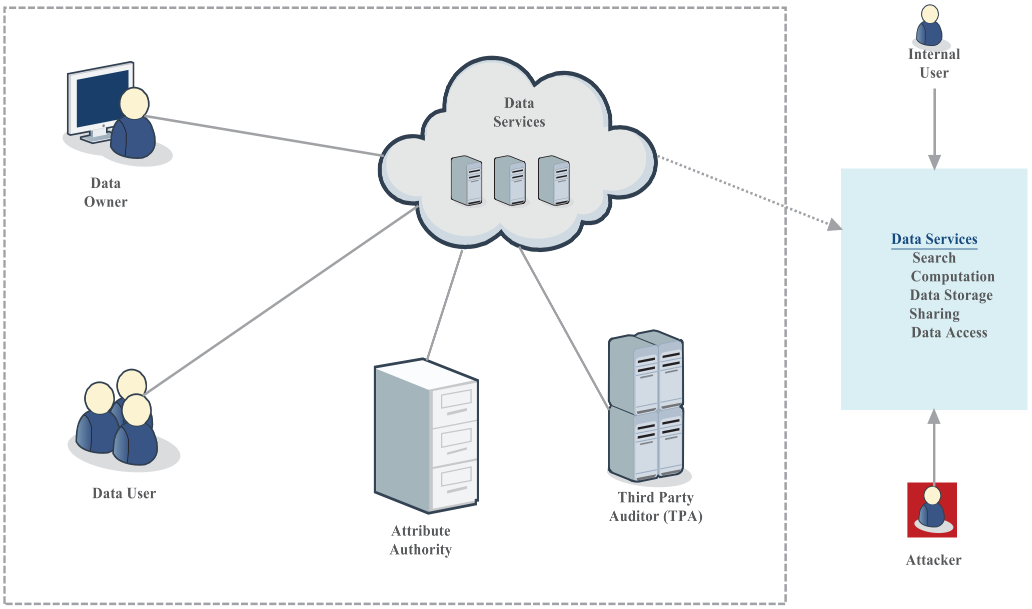

Figure 1: Model cloud framework

The third-party user may be included in providing security functions in the cloud, based on the TPA and the authority. The authority is responsible for generating the attribute keys based on the customer identity and blocking the malicious users based on their identity. Here, the trusted third party is used to check the integrity of data that are stored on the cloud. The contributions of the proposed model are presented as follows,

i) The model enforces the Enhanced Authentication (EA) for providing complete security over the encrypted content

ii) Efficient Auditing Technique (EAT) is developed here for preventing unauthorized data access from the cloud.

iii) The model effectively handles the cloud multi-latency-based security problems overcloud.

iv) Experimentations are carried out based on several cloud security-based factors using the CloudSim Simulation Tool and the graphs were provided for evidencing the proposed model efficiency

v) The results provide the success rate for detecting and preventing malicious users and authenticating the TPA with effective detection abilities.

The cloud framework model stands represented in Fig. 1, Cloud computing has grown so ubiquitous and pervasive that we no longer appreciate the extent to which it affects our everyday lives. Every day, the typical consumer utilizes 36 distinct cloud-based services frequently without even realizing it. With so much information about the current online presence, they need to figure out to what degree a cloud computing architecture can offer us a safe experience. In the cloud framework, the data services share their information with the data owner, data users, attribute authorities, and third-party auditors (TPA). Further, the data services perform various operations such as search, computing, data storage, and sharing and data access by getting information from the user and the attacker.

The remainder of this work is arranged as follows: Section 2 deliberates the literature survey, which contains several cloud securities models that handle data security and integrity that will be shared over the cloud. The complete workflow and the procedure of the proposed model are described in Section 3. The experimentation results and evaluations were presented in Section 4 with comparison charts. The conclusion and directions for future enhancement were provided in Section 5.

2 Related Works

This section presents the existing security models in the Cloud environment. An exquisite access control framework had been designed in [8] that executed data categorization for providing data confidentiality. Moreover, the shared data have been separated into different parts for promising the security of shared data. In a typical cloud model, the infrastructure is shared among others via Internet, while facing issues such as data integrity, confidentiality, fine-granularity, and scalability. In [9], Cipher-text Policy Attribute-based Encryption (CP-ABE) has been developed for providing efficient access control on the cloud, while there is a prerequisite for trusting the third party. Based on the model developed in [10], the cloud model is used for sharing the medical data on the CSP. Nevertheless, there are numerous security glitches in retrieving medicinal data from unauthorized servers. For guaranteeing data safety, the individual health record of the patient stood encrypted with Attribute-based Encryption (ABE). Further, the key management processes were performed based on the multiple authority schemes. The process of establishing a specific requirement to maintain the security of cryptographic keys in an organization is known as key management. The generation, exchange, storage, deletion, and updating of keys were all handled through key management. Another work presented in [11] discussed the online medical data sharing method, which requires higher data access and storage to be shared on the cloud. The model was developed based on the single authority manner for data access.

Valuable and efficient survey work has been presented by the authors in [12]. The paper discussed several security measures, issues, and solutions on the cloud. The Privacy-preserving cloud model solutions were developed from theoretical proposals to existing cryptographic models. The authors [13] discussed the common cryptographic models such as Arithmetic Encryption Standard (AES), Message Digest (MD), Secure Hash Algorithm (SHA), and so on. SHA's were a class of cryptographic algorithms used to protect information. It translates data using a hash function, which is a bitwise procedure, segmental additions, and solidity methods. The hash function produces a fixed-length string that has no similarity to the original. These approaches are one-way functions, which means that after they've been transformed into hash values, it's extremely difficult to return to the original data. The authors managed the encryption of the cloud storage model along with the privacy-preserving techniques that are not been processed. The pairing-based Signature Model has been presented in [14], enforced secure auditing using TPA. Moreover, the model used the batch verification technique to avoid the message overhead from the server and the cost-effectiveness of the model.

The model discussed in [15] provided the authentication protocols that provide lively data processing. Moreover, the model defines the problem of providing a parallel community auditing model and dynamic data processing for distant data processing. The work provided in [16] defines the need for a secure and unsigned communication model. Moreover, the model has not defined any cryptographic solution. Differently, a non-cryptographic solution providing user privacy in the cloud model is presented in [17]. The model derived a client-based privacy admin that minimizes the leakage factor of the private data of users [18]. Furthermore, the redundancy models are dependent on the redundancy models incorporating an Information Dispersal Algorithm (IDA). However, the solutions are not sufficient for customer linkability in detecting unauthorized user identities. The work carried out in [19] developed an anonymous and reliable access model to the cloud based on the ring and group-based signatures.

In the work [20–22], a security framework based on Zero-knowledge evidence provides anonymous authentication for new consumers. But, the major limitation of the model is the communication overhead. And, the work [23] provided a cryptographic model to assure anonymous user access to data and the security of sensitive data in the cloud model. The user anonymity and unlinkability in cloud models are processed and discussed based on group signature models. An anonymity network allows users to browse the Internet while preventing any tracking or tracing of their identities. Anonymity networks make traffic analysis and network monitoring difficult, if not impossible. Unlinkability of two events occurring during a process under the scrutiny of an attacker is the characteristic that the two occurrences appear to the attacker after the process precisely as connected–or unrelated–as they did before the process started [24–26].

Some organizations and consumers are beginning to exchange data on cloud servers as a result of the fast expansion of cloud computing technologies. To protect the integrity of unique data security in the cloud and outsourced data, this study presents the Privacy Preserved Knowledge Security Approach (PPDSA). Efficient Authentication Technique (EAT) will be used to preserve privacy throughout this inquiry, therefore cluster signing technology will be used in partnership with a third-party auditor (TPA). The auditor's job is to keep the information safe and accurately report it. EAT also harms attackers, such as cloud service providers (CSPs), and thereby knowledge users (DUs).

3 Proposed System

The proposed model contains five phases, as presented in Fig. 2. The phases are,

i) Initialization

ii) Cloud Consumer Registration

iii) Authentication based on Anonymous Access

a) Group Signature-based EAT

iv) Secure Cloud Communications

a) TPA

v) Phase of Revocation

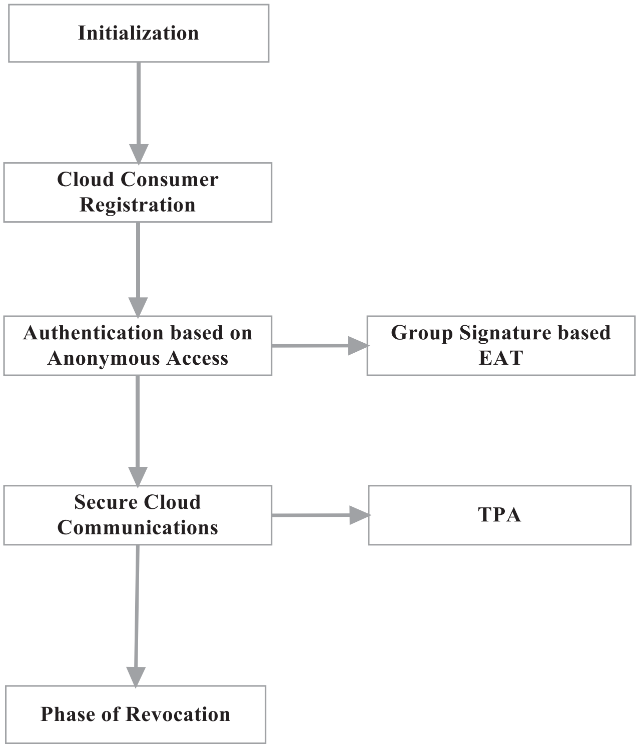
Initialization
Cloud Consumer Registration
Authentication based on Anonymous Access
Group Signature based EAT
Secure Cloud Communications
TPA
Phase of Revocation

Figure 2: Phases in the proposed model

For efficient authentication and privacy-preserving, the model uses a triangular structure, which contains Cloud Consumer, Cloud Service Provider, and Third-Party Auditor (TPA), as in Fig. 3. A cloud service provider (CSP) is an establishment providing a cloud-based platform, infrastructure, application, and storing services. Firms often only have to pay for the number of cloud facilities they use, alike to how a household would wage for a utility like electricity or gas, whereas a cloud customer is an individual or organization that has a marketable connection with a cloud benefactor and munches their amenities. Whether it's Software, Platform, or Infrastructure as a Service, the end-user is the one who utilizes the service. The model provides to assure the data integrity of the consumer data that are shared over the cloud, which can be retrieved by the users at any time based on their demands. The phases involved in the proposed model are represented in Fig. 2, where the process started with initialization, then the input data is processed in cloud consumer registration. Further, the registered data is processed in Anonymous access for authentication also it is processed in Group signature-based EAT. Where the authenticated data is processed in secure cloud communications and the third-party auditor (TPA) to determine the Phase of revocation.

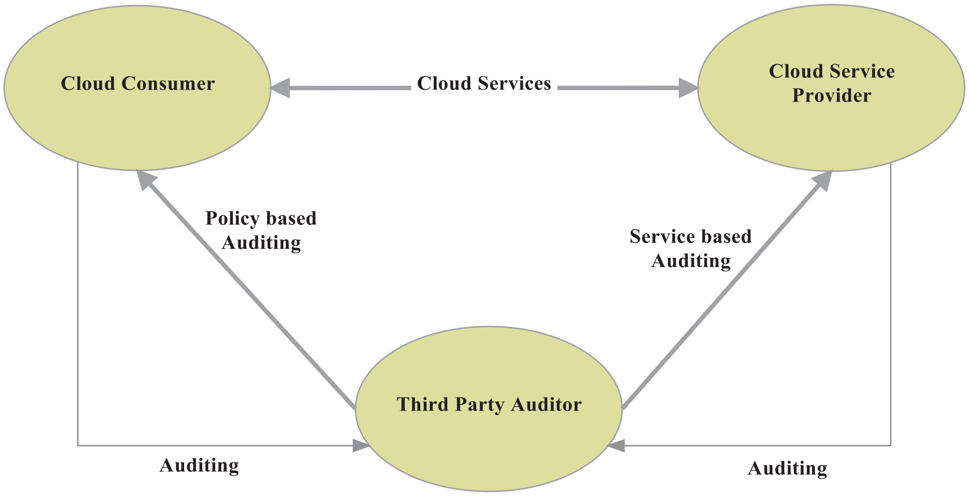

Figure 3: Triangular structured communication model

Moreover, the work focuses on measuring the reliability of the Cloud Service Provider based on the safety and privacy measures. And, the work process in each phase is explained as follows.

3.1 Initialization

Here, the initialization operations are executed by the CSP and the RA called Revocation Admin. The Cloud Service Provider produces a group 'G', contains large prime values 'm' with generators, b_1, b_2 of prime order 'm' and $m|n-1$. Additionally, the service provider generates the key pair using RSA and stores their private key as pk_{cs} on cloud. The RA produces a generator as,

$$\begin{cases} b_1 \epsilon_R Z_p^* \; of \; ord(b_1 \;\; mod \;\; r^2) = r(r-1), \;\; in \; Z_{r^2}^* \\ \qquad\qquad ord(b_1) = rr' s', \;\; in \; Z_p^* \end{cases} \tag{1}$$

where r and s are the large prime numbers. Then, the revocation admin generates the Identity Evidence (IE) for authentication, which is publicly defined. In this work, the RA is allowed to produce more than one IE based on the demands. And, the Identity Evidence set is given as $\{I_E^1, \ldots, I_E^k\}$ computed from $\{S_1^1, \ldots, S_1^k\}$, based on different consumers of cloud services.

The revocation admin further produces the generator as in the following Eqs. (2) and (3).

$$b_2 = b_1^{s_2} \; mod \; k \tag{2}$$

$$b_3 = b_1^{s_3} mod \; k \tag{3}$$

Further, the secret key for revocation (sk_r) is shared and also the other cryptographic parameters have been also generated and shared at this phase.

3.2 Cloud Customer Registration

In this phase, the cloud consumers are registered on to the CSP and request a public key that can be used for the data access of the cloud services. Initially, the consumer 'C' should be registered on the Cloud and then, the CSP verifies the user identification. Then, 'C' produces the secret rates v_1, v_2 and defines the function as,

$$C_{CS} = b_1^{v_1} \; b_2^{v_2} \; mod \; m \tag{4}$$

The consumer 'C' digitally verifies the 'C_{CS}'. Following, the 'C' requests for a public key from RA. 'C' computes $I_E^1 = b_1^{v_1} \; b_2^{v_2} \; mod \; k$ and transmits that to the cloud service provider. The generation of verification pattern as, $VP\{v_1, \; v_2 : C_{CS} = b_1^{v_1} \; b_2^{v_2} \wedge I'_E = b_1^{v_1} \; b_2^{v_2}\}$ to the revocation admin is determined. For avoiding the collusion attack, the consumer's v_1, v_2 is not accessible, since it is stored in cloud memory. Moreover, the consumer cannot have their public key, since RA only knows about the key. Any legitimate user can request the secret key or IE for authenticating themselves to the cloud.

3.3 Authentication Based on Anonymous Access

In this phase, the problem of anonymous access to the cloud is defined effectively. The major two functions involved in this work are, providing Authentication (C_i) and providing a secret key amongst the Cloud User and CSP.

i) C_i produces a random rate $rr\epsilon R \; \{0, \; 1\}^{\beta_{sym}}$. And, the factor '$\beta_{sym}$' denotes the key_size of the symmetric cipher.

ii) The random number rr was encrypted by 'C_i' using the public key of RSA.

iii) The encrypted key Enc_PK_{rr} is signed by the IE model using a group signature that ensures the authentication for consumers. Here, it is considered that the cryptographic functions such as m, $n, \; b_1, \; b_2, \; b_3, \; h_1, \; h_2$ and the IE is defined as,

$$I_E^i = b_1^{v_1} b_2^{v_2} b_3^{v_{RA}} \; mod \; n \tag{5}$$

Which are made as public and h_1, h_2 are the secure hash key. For evidencing the knowledge of the private key and signature, 'C_i' performs the IE model as below.

$$\overline{I_E} = b_1^{v_1} b_2^{v_2} b_3^{v_3} \; mod \; n \tag{6}$$

And, the ciphertext is given as,

$$C = H(Enc_{PKrr}), \; I, \; \bar{I}, \; \overline{I_E}, \; c_1, \; c_2, \; \overline{c_1}, \; \overline{c_2} \tag{7}$$

Finally, the signature factors $I, \; \bar{I}, \; \overline{I_E}, \; c_1, \; c_2, \; \overline{c_1}, \; \overline{c_2}$, and '$Enc\_PK_{rr}$' were transmitted to the CSP as the request message.

iv) The CSP checks the signed request model which comprises the significant factors such as Enc_PK_{rr}, $I, \; \bar{I}, \; \overline{I_E}$. Then, the CSP verifies for the authentication verification.

v) Then, the decryption the Enc_PK_{rr} by its private key for obtaining the random number.

vi) The CSP transmits the response message to the consumer 'C'

3.4 Secure Cloud Communications

When the previous phase of anonymous authentication is a success, the consumer ‘C_i’ can upload their data to the cloud and can be downloaded, if there is a demand. Anonymous authentication allows people to access one’s Web or FTP site’s public parts without requiring them to enter a user name or password. Moreover, the data integrity can be secured with the symmetric cipher. And, the encryption and decryption are processed here with AES in the authentication phase. Here, ensuring secure cloud communication is developed by considering that the CSP is the third-party auditor in some cases. The malicious user can be one of the third-party auditors. Hence, their illegal access to the cloud data is to be unsuccessful. Moreover, the overall process of cloud communication over in the proposed model of privacy-preserving is provided in Fig. 4, the data taken from the model is computed, and then the computed data is again processed in application service via operation model for key generation. Meantime, the generated key is given to the CSP interface for third-party administration (TPA) via Access permission and data upload. A Third-Party Administrator (TPA) is a service company that, under the terms of a service agreement, performs several services to the insurance business. The TPA is primarily responsible for ensuring data integrity. It performs tasks such as producing hashes for encrypted blocks received from the cloud server, concatenating them, and generating signatures on them. It then analyzes both signatures to govern whether or not the information saved in the cloud has been tampered with. Further, the data from the TPA is given to the cloud consumer.

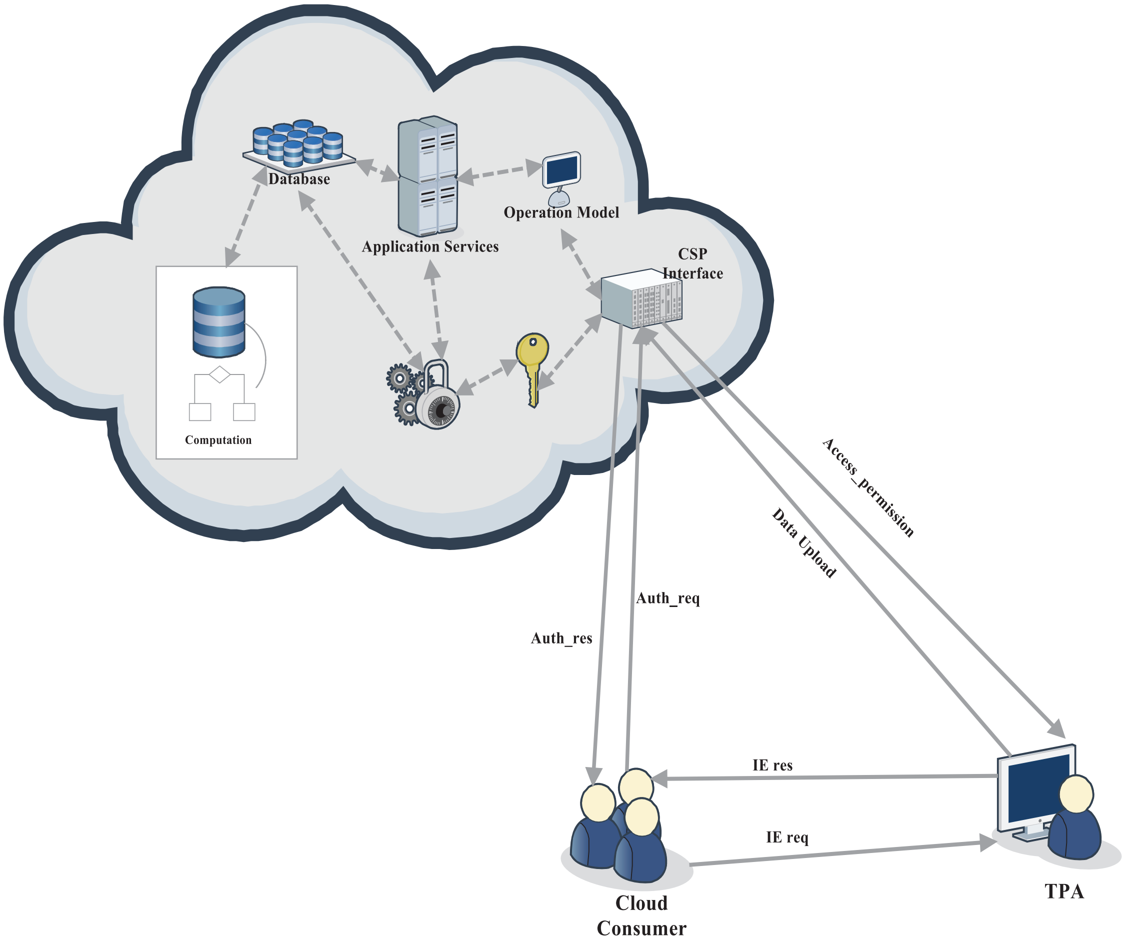

Figure 4: Model of privacy-preserved data security approach

When data is exchanged or communicated between multiple parties, it is necessary to give security to that data so that other parties are unclear of what data is conveyed between the original parties. Data security states the process of shielding data from illegal access and fraud throughout its life cycle. Data encryption, hashing, tokenization, and key management were all data security solutions that protect information across all applications and platforms.

It is considered that 'ρ' was the shared data file of the cloud consumer that comprises of 'm' number of chunks called $m = \{k_1, k_2, \ldots, k_m\}$. The cloud consumer selects the authentication_message A_M, which is given as,

$$A_M = \left[\left(\iiint_{r=0}^{m} \Delta s_r + (\log_2 L)^m\right)\{a,\ b(\nabla\alpha\beta)\}\right] \tag{8}$$

where, 'r' is the random number allocating the initial value to '$\nabla\alpha\beta$', and 'a, b' are the randomly selected rates with different lengths. Further, the mod derivation is applied for securing the shared data as,

$$A_M = \left[\left(\iiint_{r=0}^{m} \Delta s_r + (\log_2 L)^m\right)\left\{t\ (z).\frac{\Delta d}{\Delta dz}f(z) + \frac{\Delta d}{\Delta dz}t(z).f(z).(\nabla\alpha\beta)\right\}\right] \tag{9}$$

Here, the secured data is given as 'z' and the differentiation function of '$f(z)$' is needed for concealing the data and the file length. When a consumer is considered or noted as a legitimate one, then, the replica of $\nabla\alpha\beta$ is produced at the CSP. Further, the CSP needs to check the produced authentication_message of the consumer. Here, the authentication_message was framed by using the aggregation function as in the following equation. An aggregate function allows users to do a computation on a collection of data and return a single scalar value.

$$A'_M = \prod_{i=1}^{m}(\nabla\alpha\beta)C_i \le \sum_{n=0}^{\infty}(\nabla\alpha\beta)^N \tag{10}$$

where, '$(\nabla\alpha\beta)^N$' is the aggregated rate. When the authentication _message of the consumer matches with the aggregation function of the service provider, the cloud consumer is considered as a legitimate user in the particular cloud paradigm. Then, the third-party auditor obtains the private key from the service provider considering the authentication message of the consumer for initiating the process of privacy-preserving through auditing. Cloud Audit is a standard established by the CSA in 2019 for presenting information about how a cloud service provider handles control frameworks. Cloud Audit's purpose was to give cloud service providers a method to make their performance and security data more accessible to potential customers. In the process of each auditing, session keys are needed by the auditor for verification. And, the flow is presented in Fig. 5.

The auditing process is initiated when the auditor produces a sample verification message called 'M_v' against each service to the consumer to verify that the services are provided from the legitimate CSP. The selects a random rate '$\forall\partial$' for all the obtained cloud services, $c_s = \{s_1, s_2, \ldots, s_n\}$. The factors in each service are different from one another and the CSP is verified with the M_v. Based on the factors, the authentication is verified with the TPA to provide the services to the consumer's insecure manner.

3.5 Phase of Revocation

Based on the verification results, the revocation process is processed, in which the consumer can be revoked when they fail to prove their authenticity to the cloud. The process is carried out with the Revocation Admin (RA). In the cloud, user revocation is the most challenging since the revocation of one user affects others who share the same attribute space. Broadcast CP-ABE is a direct revocation architecture, which allows for fine-grained revocation without harming non-revoked users. There are numerous sorts of revocation processes, including direct and indirect revocation, as well as single-user and multiple-user revocation. Initially, the RA derives the random session key and the contribution rate of the private key as 'v_{RA}'. Then, the v_{RA} broadcasted into the block queue. When the consumer is revoked from the framework, they are denied to access the cloud services.

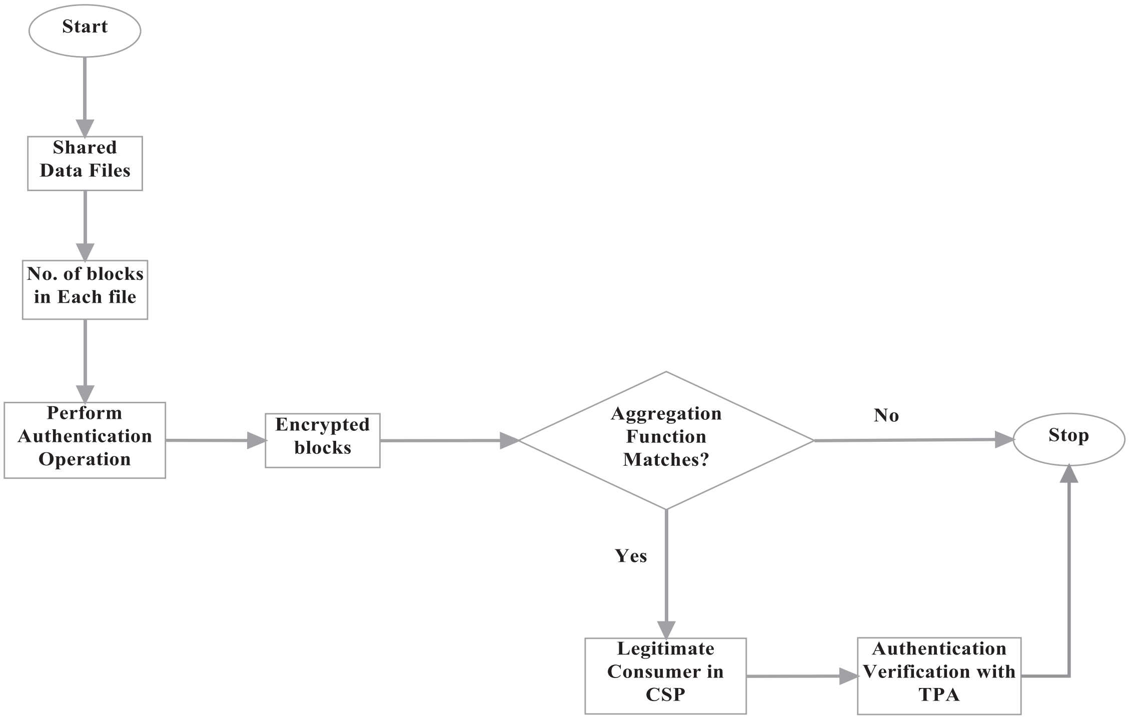
Start
Shared Data Files
No. of blocks in Each file
Perform Authentication Operation
Encrypted blocks
Aggregation Function Matches?
No
Stop
Yes
Legitimate Consumer in CSP
Authentication Verification with TPA

Figure 5: Process of authentication verification for privacy preserved communication

4 Experimental Results and Evaluations

The performance of the proposed Privacy-Preserved Data Security Approach (PP-DSA) evaluated in this section using the simulation tool called Network Simulator 2 (NS2) and Cloud Sim. Moreover, the model is analyzed with different cases comprising three entities as CSP, Cloud Consumer, and TPA. The following parameters were considered for the testing and evaluations process.

i) Model Effectiveness
ii) CSP Reliability
iii) Functional Efficiency
iv) Processing Time

Model effectiveness: Accuracy, precision, and recall were the three elementary actions used to assess a classification model. The proportion of correct calculations for the trial data is known as accurateness. It's modest to dig it out just by separating the number of right conjectures by the total number of predictions.

CSP Reliability: A Service Level Agreement (SLA) is made with the CSPs in which they will agree to deliver on-demand service requests to the user and with utmost security to deliver to the end-users. A CSP is a corporation that delivers some component of cloud computing to other establishments or individuals, often, when searching the internet, a cloud service is characterized as Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Platform as a Service (PaaS).

Functional efficiency: Cloud efficiency is the capacity to make the greatest use of cloud resources at the lowest feasible cost with the smallest quantity of waste and unnecessary efforts.

Processing time: The processing time is calculated using the file size as a variable in this paper.

The obtained results are compared with CP-ABE and Anonymous Authentication Model. Concerning that time, the computation overhead is computed at the process of proposed key generation and key sharing through the defined model. When storage overhead is assumer, the proposed security model is very much important to process the originally shared data with the generated keys. The following Tab. 1 presents the results of key generation time obtained between models. It is obvious from the Fig. 6 that the proposed model attains a minimal rate of key generation time than the existing model, which may reduce the communication overhead effectively and increase the processing speed in providing services to legitimate consumers through the cloud. The time required to generate a key analysis of the proposed method is shown in Fig. 6, where the key generation time investigation of the proposed model is compared through existing models in which the rate of key generation time is lesser than the existing model and it also reduces the communication overhead effectively.

Table 1: Results for key generation time

Models	10	20	30	40
PP-DSA	5.12	3.9	8.0	14.1
CP-ABE	6.7	5.0	11.0	18.0
Anonymous authentication	7.2	7.7	12.19	18.28

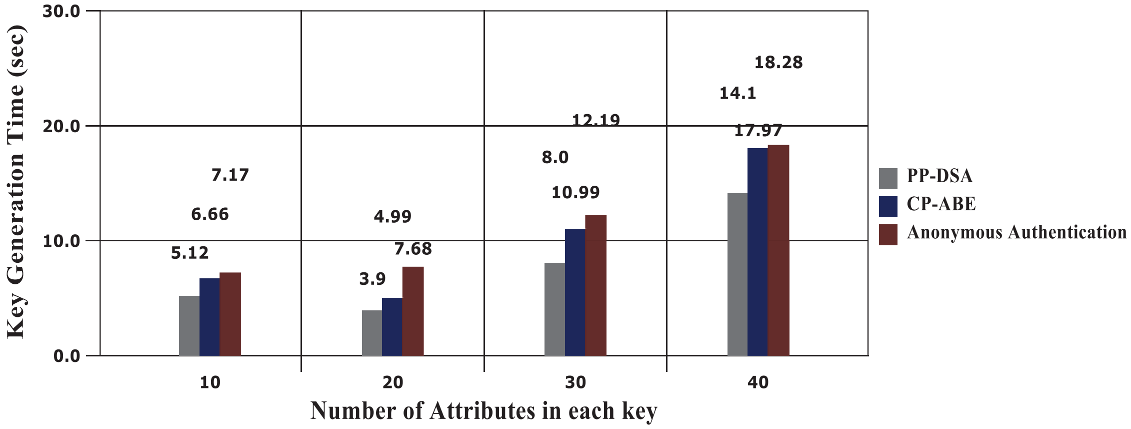

Figure 6: Key generation time analysis

The model execution time is another significant factor to be evaluated for evaluating the effectiveness of the proposed model. Here, the processing time is analyzed for the file size. Fig. 7 shows the result of the execution time and the equivalent outcomes are provided in Tab. 2.

The proposed privacy-preserving model analysis comprises the evaluation of the security level of the model. The cloud services provided by the CSP to the cloud consumers insecure manner based on time are evaluated and the results are portrayed in Fig. 8. The effective implementation of the secure design makes the model provide a higher rate of services to the cloud users based on their demands, which is evidenced in the following Fig. 8. With the proposed model, as in the following chart, the model provides 97.8% of services to the consumers effectively.

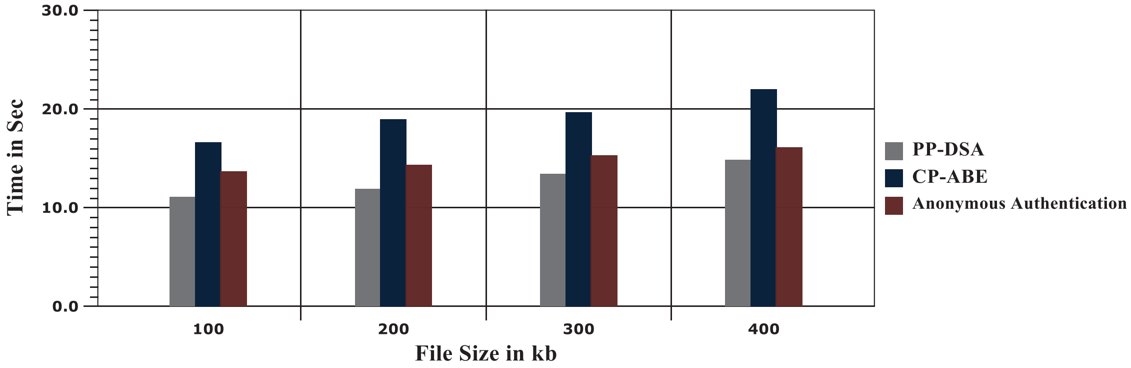

Figure 7: Comparison chart for execution time analysis

Table 2: Time effectiveness results

Models	100	200	300	400
PP-DSA	11.01	11.83	13.35	14.81
CP-ABE	16.54	18.91	19.6	21.94
Anonymous authentication	13.64	14.29	15.24	16.07

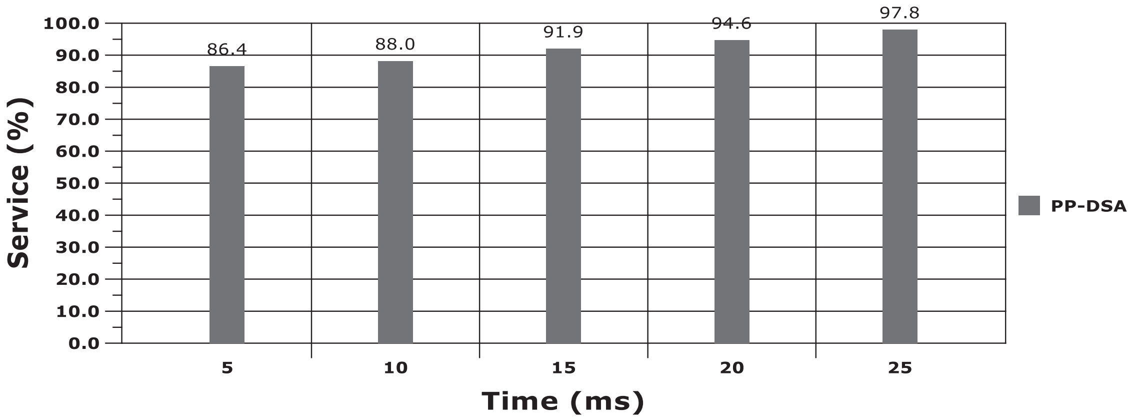

Figure 8: Cloud services *vs.* time

Further, the total time that is taken for encryption and decryption operations are computed and the obtained values are given in Tab. 3. Here, the encryption and decryption time for securing the secret key and shared files are evaluated and the average rates are plotted against the number of files. The effective utilization of the phases in defining the privacy-preserving cloud model reduces the time taken for concealing the shared data using encryption and decryption operations and the results are displayed in Fig. 9. This enhances the model effectiveness by allocating or providing the services to the consumer in the fastest manner than other compared models.

Table 3: Values obtained for encryption and decryption time evaluations

Number of files	20	40	60	80	100
Encryption time of PP-DSA	24.4	24.5	25.8	29.4	33.4
Decryption time of PP-DSA	19.5	20.8	22.3	23.3	28.7
Encryption time of CP-ABE	15.1	18.4	16.0	18.2	21.9
Decryption time of CP-ABE	10.0	10.0	11.3	10.0	13.3
Encryption time of anonymous authentication	4.9	5.2	8.1	8.1	10.6
Decryption time of anonymous authentication	−1.3	−0.6	2.9	3.0	5.1

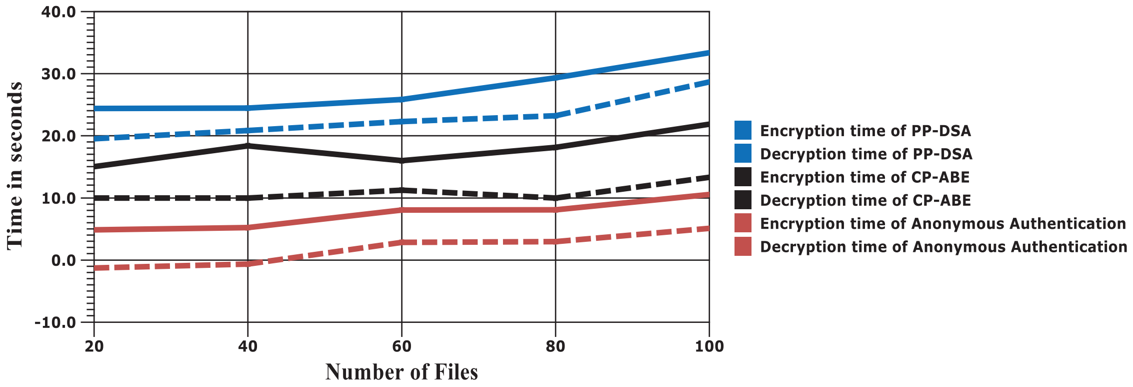

Figure 9: Time-based evaluations for encryption and decryption

The reliability of the cloud service provider is an important concern in the defined model. While considering the reliability, it is determined based on how the consumer data are secure in the cloud and effectively delivered based on demands. In the following Fig. 10, the results obtained for the measure of model effectiveness are plotted based on the number of services provided through the model. Concerning the number of auditing, the proposed model achieves a higher rate of effectiveness than the compared works. And, the values obtained for the effectiveness measurement are presented in Tab. 4.

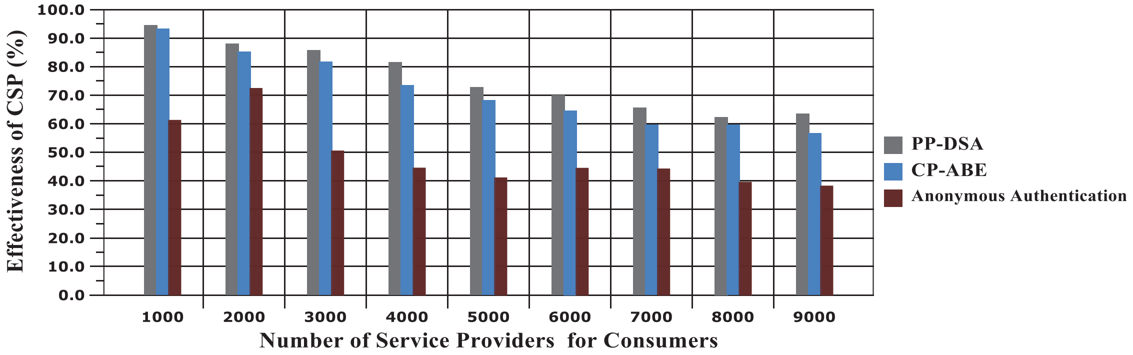

Figure 10: Effectiveness of CSP results

Table 4: Values obtained effectiveness measure

Models	1000	2000	3000	4000	5000	6000	7000	8000	9000
PP-DSA	94.42	87.82	85.66	81.34	72.59	69.83	65.51	62.21	63.35
CP-ABE	93.1	85.06	81.64	73.31	68.03	64.49	59.51	59.45	56.57
Anonymous authentication	61.19	72.41	50.45	44.45	41.03	44.39	44.15	39.47	38.15

5 Conclusion and Future Work

To ensure data confidentiality in the cloud model, it is necessary to develop a novel model to authenticate the three elements, such as Cloud Consumer, Cloud Service Provider, and Third-Party Auditor (TPA). Another important model is to develop a privacy-preserving model to limit the vulnerabilities and prevent the data from external threats. In this paper, Privacy-Preserved Data Security Approach (PP-DSA) is developed to provide data integrity and privacy-based issues among the cloud elements. The model comprises five phases, namely, initialization, cloud consumer registration, Authentication for anonymous access using the group signature based on EAT, secure cloud communications with the TPA, and Revocation. For EAT incorporation, group signature is used with bilinear pairing functions, and secure communication is provided with effective auditing in TPA. The results show that the model provides a better rate of security than the compared models. The proposed model provides 97.8% of cloud services to consumers effectively based on their demands.

In the future, the model can be further developed with a higher rate of security operations with advanced cryptographic functions and algorithms. The model can also be implemented and experimented with within a real-time environment.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Rajkumar, C. H. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–61, 2009.

[2] M. Peter and T. Grance, *The NIST Definition of Cloud Computing*, Gaithersburg, MD: Special Publication (NIST SP), National Institute of Standards and Technology, 2011.

[3] U. Premarathne, "Hybrid cryptographic access control for cloud-based EHR systems," in *IEEE Cloud Computing*, vol. 3, no. 4, pp. 58–64, 2016.

[4] C. Esposito, A. Castiglione, C. A. Tudorica and F. Pop, "Security and privacy for cloud-based data management in the health network service chain: A micro-service approach," in *IEEE Communications Magazine*, vol. 55, no. 9, pp. 102–108, 2017.

[5] R. Sumant, M. Eloff and E. Smith, "The management of security in cloud computing," in *IEEE Information Security for South Africa (ISSA)*, vol. 1, pp. 1–7, 2010.

[6] C. Yong, R. Buyya and L. Jiangchuan, "Cloud computing. China communications," in *China Institute of Communications (CIC) and the IEEE Communications Society (IEEE ComSoc)*, USA, 2014.

[7] A. N. Toosi, R. N. Calheiros and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Computing Surveys*, vol. 47, no. 1, pp. 1–47, 2014.

[8] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. of the 29th IEEE Int. Conf. on Computer Communications*, USA, pp. 534–542, 2010.

[9] K. Yang and J. Ziaohua, “DAC-MACS: Effective data access control for multi-authority cloud storage systems,” *Security for Cloud Storage Systems*, vol. 1, pp. 59–83, 2014.

[10] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[11] M. Li, S. Yu, K. Ren and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in *Int. Conf. on Security and Privacy in Communication Systems*, Singapore, pp. 89–106, 2010.

[12] H. Guo, Z. Zhang, J. Zhang and C. Chen, “Towards a secure certificateless proxy Re-encryption scheme,” in *Springer: Int. Conf. on Provable Security*, Berlin, Heidelberg, pp. 330–346, 2013.

[13] Y. Chen and R. Sion, “On securing untrusted clouds with cryptography”, in *Proc. of the 9th Annual ACM Workshop on Privacy in the Electronic Society*, New York, ACM, pp. 109–114, 2010.

[14] C. Wang, “Privacy-preserving public auditing for data storage security in cloud computing,” in *INFOCOM 2010 Proc. IEEE*, San Diego, march, pp. 1–9, 2010.

[15] Q. Wang, “Enabling public auditability and data dynamics for storage security in cloud computing,” *Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[16] R. Laurikainen, “Secure and anonymous communication in the cloud,” in *Aalto University School of Science and Technology*, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, Finland, pp. 1–5, 2010.

[17] M. Mowbray and S. Pearson, “A Client-based privacy manager for cloud computing,” in *Proc. of the Fourth Int. ICST Conf. on Communication System Software and Middleware, ser. COMSWARE ‘09*, New York, ACM, pp. 1–8, 2009.

[18] E. M. Hernandez-Ramirez, V. Sosa-Sosa and I. Lopez-Arevalo, “A comparison of redundancy techniques for private and hybrid cloud storage,” *JART Journal of Applied Research and Technology*, vol. 10, no. 6, pp. 1–9, 2012.

[19] M. Jensen, “Towards an anonymous access control and accountability scheme for cloud computing,” in *Cloud Computing (CLOUD), 2010 IEEE 3rd Int. Conf. on Miami*, IEEE, USA, pp. 540–541, 2010.

[20] P. Angin, “An entity-centric approach for privacy and identity management in cloud computing,” in *Reliable Distributed Systems, 2010 29th IEEE Sympo. on New Delhi*, IEEE, India, pp. 177–183, 2010.

[21] C. Gokulnath, M. K. Priyan, E. V. Balan, K. P. Rama Prabha and R. Jeyanthi, “Preservation of privacy in data mining by using PCA based perturbation technique,” in *2015 Int. Conf. on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, India, pp. 202–206, 2015.

[22] P. N. Hiremath, J. Armentrout, S. Vu, T. N. Nguyen, Q. T. Minh *et al.,* “Mywebguard: Toward a user-oriented tool for security and privacy protection on the Web,” in *Int. Conf. on Future Data and Security Engineering*, Vietnam, pp. 506–525, 2019.

[23] R. Lu, “Secure provenance: The essential of bread and butter of data forensics in cloud computing,” in *Proc. of the 5th ACM Sympo. on Information, Computer and Communications Security, ser. ASIACCS ‘10*, New York, ACM, pp. 282–292, 2010.

[24] S. Chow, “Spice–simple privacy-preserving identity-management for cloud environment,” in *Int. Conf. on Applied Cryptography and Network Security*, Singapore, pp. 526–543, 2012.

[25] N. Deepa, P. Vijayakumar, B. S. Rawal and B. Balamurugan, “An extensive review and possible attack on the privacy-preserving ranked multi-keyword search for multiple data owners in cloud computing,” in *2017 IEEE Int. Conf. on Smart Cloud (SmartCloud)*, USA, pp. 149–154, 2017.

[26] X. Boyen and B. Waters, “Compact group signatures without random oracles,” in *Advances in Cryptology-EUROCRYPT 2006*, vol. 4117, pp. 427–444, 2006.