Neural Parallel and Scientific Computations 29 (2021), No. 3, 146-160

AN EFFICIENT USER PROTECTED ENCRYPTION STORAGE ALGORITHM USED IN ENCRYPTED CLOUD DATA

ANGELIN PEACE PREETHI
Karpagam College of Engineering,
Anna University, Chennai
Email: 3jsngl@gmail.com

ABSTRACT

Cloud data security needs have become an ongoing issue that needs to be addressed urgently. The data encryption cloud is a valuable tool to ensure data security. The existing proxy server system allows many users to perform search operations to find the problem time lag and encryption of data that is not overflowing with cloud storage. Many researchers have been inspired by this work under the single data owner system and the multi-owner data system. As Protected Data Encryption Algorithm (PDEA), this algorithm is used to store data in a database provided by a single cloud service provider and cloud server to conduct data access with no actual data volume. Use simple data recovery and access procedures. Cloud storage, for companies to store data locally during this process. PDEA stores prefer active cloud storage services to lower prices and use a large amount of data to store. Cloud computing is based on rapid development and builds a secure search code from information recovery. Therefore, dual outsourcing of data in the cloud is cheaper, minimizing long-term storage and maintenance complexity. There are data integrity, reliability, security, and minimum guarantees available on the cloud server.

Keywords: Cloud Computing, Data Confidentiality, Data Integrity, Remote data verification, Visual Cryptography.

1. INTRODUCTION

Cloud computing is mainly based on data centers, owned by hosted cloud services where there are thousands of dedicated servers. In addition to the increasing number of dedicated servers parked in data centers, there are billions of unused Personal Computers (PCs), typically used by individuals and organizations around the world for just a few hours. As well as introducing general mobile cloud services to app developers and advertisers we will review

Received July 14, 2021
www.dynamicpublishers.org;
https://doi.org/10.46719/npsc20212932

the general structure of the mobile cloud with this tutorial, facts, goals, prediction system. How Mobile Cloud Computing Application Includes computing design about the industry's perfect benefits and applications, tools, advantages, and disadvantages of mobile cloud, and infrastructure. In addition, the use of online application computing opportunities and cloud challenges.

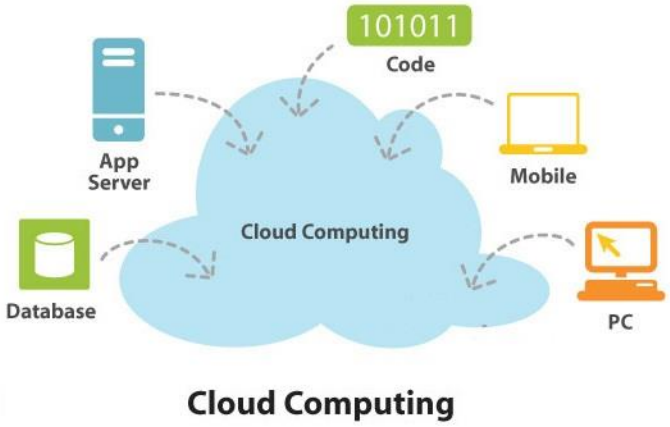

Figure 1: Cloud Structure

This cloud computing is an important challenge and it is possible to introduce some of the roles of mobile cloud applications in the design of costs, computing structures, and how the application industry has the opportunity to migrate to cloud computing systems with less investment.

Underutilized a large range of underdeveloped computing and storage capabilities of PCs can be used to replace cloud fabrics to provide a wide range of cloud services, primarily as a service infrastructure. Therefore, this method is called the "data centerless" method which completes the data centers, cloud-based rendering model. It is understood that if a company’s data is highly confidential, the business owner is definitely more concerned about putting the data in the hands of other parties. An on-campus private cloud is a viable solution to this problem.

The traditional economic capacity zoom framework should be replaced with control optimization and load control system disruption. A perron-Frobenius practical approach to organizational design and operation based on the Future Job Utilization Framework is to address the doorstep. Interestingly online measurement at the Perron-Frobenius is associated with potential capabilities the system is approaching a volatile / turning point to provide "initial

warning signals" however, setting up a private cloud infrastructure can be very costly for a data center that requires a large transparent investment. We know that cloud computing is a complex system and a number of systemic risks are associated with the potential for state system phase change.

2. RELATED WORK

Cloud paradigm, the information is stored on an outsourced server and the requested data can be retrieved by the owner. But there is no data stored securely on a remote server that is protected and not modified by the cloud service provider [1]. Default storage is also vulnerable to security attacks from these two illegal users and the CSP (cloud service provider).

Traditional encryption technology suffers from computing and storage issues. Therefore, getting ready to secure cloud storage space will be a complex but first task. Once the data is stored in the cloud, the data owner loses control over the security of the stored data. The CSP can cover unexpected loss of data or reduce data to never re-access storage data [2]. Therefore, data owners are forced to verify data integrity and data reserves in the cloud.

Many researchers have proposed various new and effective audit schemes to verify and confirm data reliability. Another notable feature of cloud data auditing is the guarantee of data privacy. To reduce his computational load a Trusted Third Party (TTP) data provider is provided with reliable, and an audit protocol has been implemented, which has been checked several times to assist in the reliability of his stored data [3]. However, another notable feature of cloud data auditing involves support for dynamic data operations.

Due to the huge increase in data storage, technology is required to obtain information and security to focus on effectively protecting these large data and data related issues. It is one of the most useful tools for extracting large amounts of information. It is a rather difficult task because of the variety of sizes and data in these situations health applications, global personal data, public sector management, etc. [4]. There is a wide range of analytical and searchable data. In order to maintain and recover data, new upgrades to the software will be in great demand.

Advise neutral public and private cloud executives and security issues and challenges. All members of the team shared confidential information about the use of this technology in national security, finance, and finance-related information [5]. In the traditional visual encryption scheme, the image is divided into a group of members to distribute multiple image shares. The original image can be obtained by combining the shares of all members. This confidential image becomes accessible to every individual member and for illegal purposes, intrusive valuable information, and any member of the group is at risk of using it [6]. Discussions on data security, data verification, data dynamics, big data processing, and extension discuss shared confidential information.

Data protection cloud Storage cloud Access without authorization is a natural desire of the customer to protect his data. If it reserves any data that is disclosed the resource is owned by the customer, the existing stability and/or authorization measures can protect the data from possession, loss, damage, or theft. However, when the data is in the hands of a third party that is, the public cloud provider, and the data will be exposed [7] [8]. This means that customers need two security envelopes: the cloud provider helps to protect the data from being attacked from the outside and also tries to prevent the data from being visible / cloud accessible.

One way to do this is to encrypt cloud data. This section will talk about this in detail. Currently, there is a large amount of literature on encrypted cloud performance. The encryption cloud is provided with high-level configuration [9]. Basically, the customer data processor processes and cloud send data and metadata (quantity, words, etc.). The key is only saved to customers. Customer Data Verification Data integrity can be verified at any time.

The Client-side performs data recovery and sends a cloud token generated by the token generator. The cloud uses the token to retrieve data encryption and send it to the customer. Then, the client uses the key to decrypt and recover the data with him. If the customer wants to grant access to other users, the token cloud can be sent to the new user to communicate [10] [11]. Such a scheme is suitable for simple storage operations. The fact that Sullivan used digital identification and control effectively underscores the legal and business importance of disclosure and disclosure.

Amazon Simple Storage Service S3 works in a similar way. S3 authentication uses encryption for its users, but the data is not encrypted by default [12]. However, the data can be formatted and stored on S3 (Google Now encrypts the cloud storage by default). Using an

encryption cloud is as well documented and discussed like this. The data is controlled and the user maintains and encrypts the encrypted data which provides a robust security framework [13]. A promising cloud is limited by the risk of accessing our data or attack from the outside.

A user-friendly storage controller and the optimized claim has been verified in real footage by many cloud service providers. The fortis method securely suggested a cloud of computing for customer store data solutions and ensure security. Since users give their confidential information to the cloud, it is always important to make sure that this information is not leaked to anyone or that the cloud service provider is misleading [14]. A hybrid approach has been proposed as a practical solution in a cloud computing system for medical document sharing as privacy is protected [15].

User information confidentiality can be achieved by applying various protocols to user data and storing cloud information [16]. Use two important encryption technologies, namely visual and quantum cryptography, to ensure that they are more secure than traditional electronic payment systems.

Remote storage Stored information can be easily corrupted, modified, or removed due to hardware breakdown or human defects [17]. Therefore, the accuracy and completeness of static data in the cloud are important. Two new schemes, such as Certificate Data Provable Data Possession (PDP) and Proofs of Irretrievability (POR), have been proposed for the purpose of level preparation [18]. The design concept of scalable and efficient PDP technology is proposed based on the ability to remotely verify data on remote servers if the data can be proven.

This protocol file is used for random data owner-selected outsourced storage verification and it only supports limited verification data and dynamic data operations. Used a social audit protocol based on the synchronous authentication bidirectional signature with the Merkele hash tree, which was developed and becomes fully dynamic data functional [19] [20]. Lazy encryption, attribute-based encryption, proxy re-encryption can lead to approved feedback access to access data. Cloud data storage system data A large number of effective data recovery solutions have been proposed.

3. IMPLEMENTATION OF PROPOSED SYSTEM

When a user intends to upload a file containing some confidential information, it must have encryption technology, including two levels. Initially, the document file should be

converted to a text file using the Apache Favorite Application programming interface. In the next step, the resulting text file will be encrypted using encryption technology.

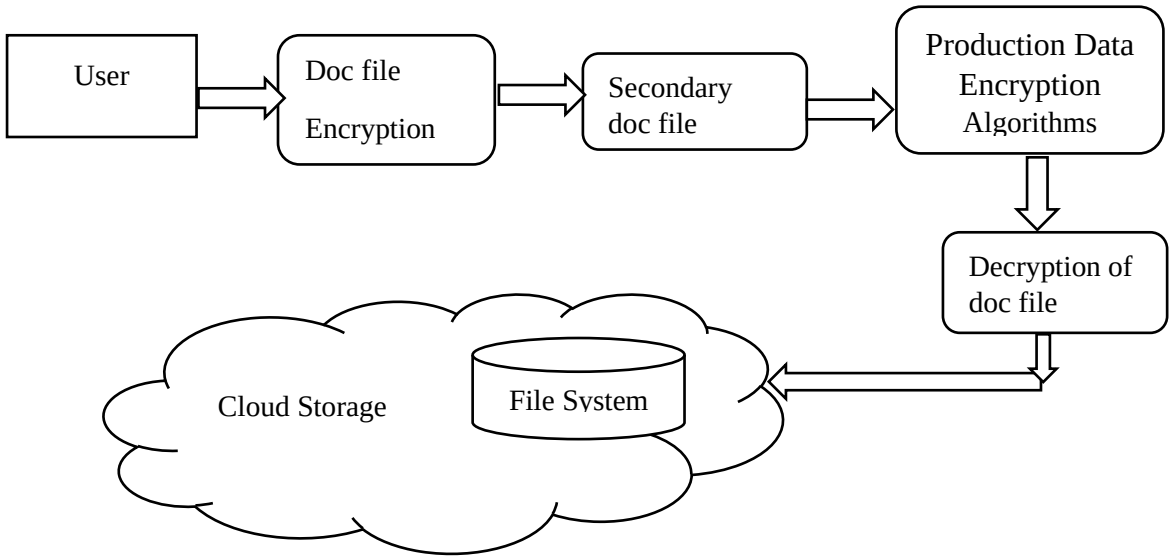

Figure 2: Block Diagram

Each line from the text file must be read and converted to an integer (ASCII value) for each character. Individual pixels should feed the repository image using the text file system. The first image of the pixels line should be placed along the sequence of the second image next to the third image. Repeat this process until about the end of the file. Finally, the image file shares with the cloud must be loaded.

Protected Data Encryption Algorithm

The cloud looks good, cloud, and data to its owner, then details outsourcing, but it can cause some data transmission problems. There may be data loss and damage by third party providers. Users who are only allowed to encrypt and decrypt access cloud data confidential data sharing are an effective realization and static data sharing using an encryption algorithm. The proposed system processing is used for convenient data access and reliability for multiple

data storage users. Cloud computing data is used to authenticate access cloud data only where it is accessed to avoid unauthorized users.

Algorithm for Conversion of original document file into text file

Input: doc/docx file

Output: Text File

Step 1. Read the document file to the file dox/ Docs extension with rama.docx

Step 2. Word document file accessed using the HWPF (Horrible Word Processor Format) document component

Step 3. Class organization. Apache. Poi. xwpf. Extractor. XPFWordExtractor extracted and returned from Word documents to simple data

Step 4. Use the available Text () function to recover all the text in the file

Step 5. Store data in the text file

Security is a major issue when users outsource their own data to the cloud. Cloud service providers can provide users with unrestricted access and information regarding authorized user access that addresses the risk of user data leakage. Therefore, all information can be safely transmitted and processed securely, the PEDA algorithm uses many problems to solve search term, short, and so on.

Algorithm for Encryption of Text file into shares

Both phases involve when the user wants to recover the original document file stored in the cloud image using PDEA decryption technology. In the initial stage, the image file is converted to a text file. From image sharing, every line in the .png format must be read using the RGB method available for every pixel from the line. The pixel should be converted to sixteen feet of code and stored in the string buffer extracted. Repeat this process until about the end of the file. Finally, all the content in the buffer must be converted to a text file, in the next step, the text file is converted to an original document file using the interface in the Apache favorite application program.

4. RESULT AND DISCUSSION

The proposed PDEA algorithm has been implemented in Java and various experiments have been implemented. Algorithmic document files are executed in various sizes; Algorithm and other data Partitioning and execution time PDEA encryption and deletion technology come with performance Symmetric algorithms such as DES and AES are tested by size parameters. In the encryption process, the image of the original document file is converted into a text file, and then one to share. File test results for the proposed PDEA technical documentation are as follows:

4.1 Conversions of the Document File into a Text File

Apache poi converts a document file into a text file using the application project interface. **Figure 2 and figure 3** shows the sample document file and the text file after conversion.

Figure 2: Sample Document File

Figure 3: Secondary Text File

Convert text files to image files to original documents using PDEA decrypt technology
The resulting image file is decoded into a text file using PDEA technology. The obtained text file is converted into a document file using the Apache POI application program interface. **Fig 3** Programs Modified Original Document File Effect.

This technology has been tested and various document files have been found in the process of encrypting the image partition size compared to the original file. Table1 is a comparison detail between text files and data partitions of different sizes, compares the file size of the original document with the image partition.

Protected Data Encryption Protocol (PDEA) mode provides multi-way balancing without load congestion. This method provides the best solution for cloud load balance in the absence of congestion.

There is an intermediate server farming system, consisting of 20 slots in the form of cloud sports aircraft used in the proposed process. They have three features related to 10-level data centers, 6-level data centers, and 4 sets up a data center. These 20 locations require more than 10,000 connections. The existing method compares to Deduplication Supporting Strong Privacy Protection (DSSPP), fair stock, greed method, and proposed Protected Data Encryption Protocol (PDEA). The resulting proposed work showed that it showed a high-level performance.

Table 1. Implementation parameter used in the proposed method

Processed Parameter	**Value processed**
No. of Parameters	4
Type of data	Data files
No. of comparison methods	4
Service provider	Cloud Service Provider (CSP)

Above **table 1,** the defined values and flow analysis parameters are shown in the proposed method. Test parameters include resource allocation, congestion rate, critical time, and network usage. These test boundaries of this strategy are compared to existing strategies for duplicating data security strategy data capability and firm privacy protection support.

4.2 Data Transfer Ratio

This strategy is comparable to the data transfer rate and the current strategy is Data Protection Strategy, a data backup technology that supports robust privacy protection and DSSPP. The proposed work produces more productivity than different technologies.

Data Transfer Ratio Speed = (Amount of data /Transfer Time)*100

Table 2: DATA TRANSFER in %

	Data Transfer %		
No of Files	**DSP**	**DSSPP**	**PDEA**
10	25	33	41
20	30	40	50

30	40	50	58
40	55	60	66
50	65	68	83

The effective result of **Table 2** proposed scheme for resource allocation is about 83% of firm privacy protection and information records data backup, of values for the existing method DSSPP 68% and DSP 65%. One of the currently proposed calculations for outflanks to make the resources are available.

Figure 4 screen shots

Fig 4 The result is that the method proposed in the example gives the most consistent implementation of the PDEA test range, resource allocation, congestion rate, unpredictable high response time, and are all highly skilled considered to use the network.

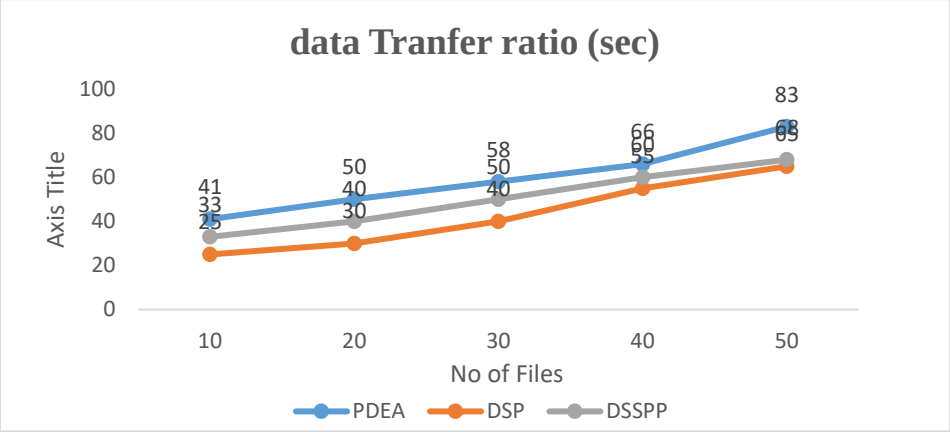

Figure 5: Data transfer ratio

Fig 5 Data transmission ratio efficiency based on data transmission over shows. In this picture, the existing and presented methods are compared; High efficiency resulting in shows 95%. It suggests that one of the recommendations is better than the existing one.

Data loss rate:

The existing methods of congestion rate in the proposed work are compared with the amount of data loss (PDEA). Compared to the existing methods, the effectiveness of the proposed method will increase performance.

$$L=10n\log_{10}(D) * A$$

Where, L is the path loss in decibels, n is the path loss exponent, D is the distance between the transmitter and the receiver, and A is an Amount of data

Table 3: Data loss rate

No of Files	DSP	DSSPP	PDEA
10	45	40	30
20	50	44	34
30	52	48	36
40	62	52	38
50	65	58	40

Table 3 Includes the number of completed moves per unit time for system use. The time it takes to complete the transmission of data is called the transmission completion time. The methods to be compared are DSSPP, DSP, and the proposed PDEA.

Figure 6: screen shots

Fig 6 The proposed framework will be used to evaluate data transfer between data centers for backup for future use. Implemented by Visual Studio Framework 4.0.

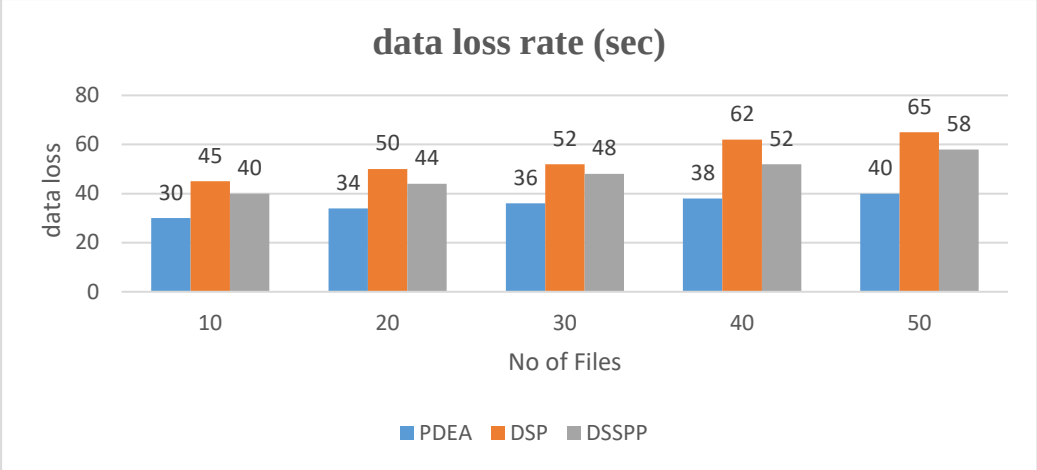

Figure 7: Analysis of data loss rate

Fig.7 the programs in figure 5 above increase the output by comparing the data loss rate between proposed and existing methods. The number of PDEA moves, and a positive result decreases compared to the current structure and increases the time to reach. The end time for 100 data information moves is 24secs for the stated strategy and 21secs for DSSPP. While the existing method implementation is incredibly low, the number of proposed it gives high performance.

Time complexity

The time complexity is the proposed system and the data transfer time is taken to be very low time compared to other methods. The existing technology is dsspp, and DSP, proposed PDEA.

Table 4: Time complexity

No of Files	DSP (MS)	DSSPP(Ms)	PDEA(Ms)
10	45	40	30
20	50	44	34
30	52	48	36
40	62	52	38
50	65	58	40

Table 2 Number of completed transfers; the proposed scheme is 20 ~ 45secs. Transfer completion time is reduced and data transfer volume is expanded. For more information on its purpose, the movement was completed in a short time.

Figure 8: screen shot

Fig 8 Ranked number one in the rankings, while at the same time the number exchange satisfaction time with the increase in information movement is low. The test range is highly activated under test conditions.

Time complexity T (n) = n - 1 ≤ 1 in Msec

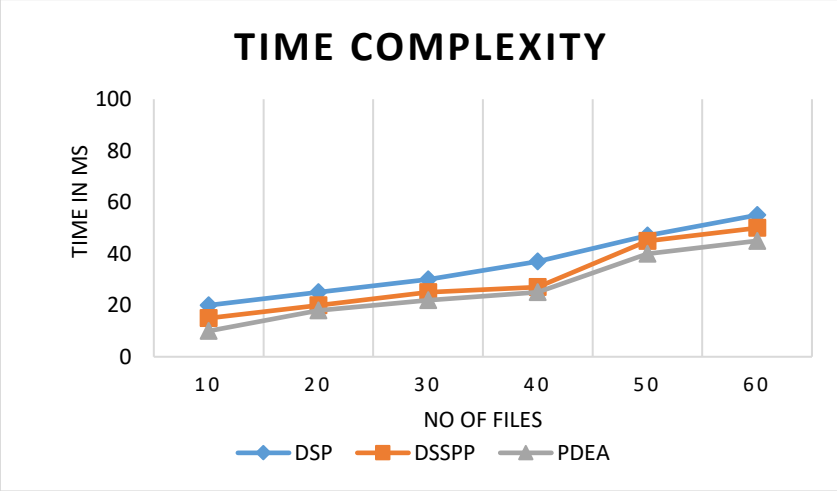

Figure 9: Analysis of Time Complexity

Fig 9 of the above shows the time complexity of existing and proposed methods. The time taken to transfer data using the proposed method is 0.1 seconds, which is very short. While the existing method gives the result 65% In terms of transport delivery, the time it takes to complete the job is very effective compared to other methods.

5. CONCLUSION

The proposed technology is to achieve data privacy in the PEDA Cloud computing system. Cloud service providers are considered unreliable, the data should not only come from external attacks, but the cloud provider is hidden. Keeps secret from the cloud Extraction of information is impossible. Overhead key management using conventional systematization technology involves an increase in demand, quantity, time, and calculation resources 65%,58%,40% The complexity in our system is far less than the fair and standard algorithm. PDEA technology ensures data confidentiality and security, along with integrity and reputation.

REFERENCES

[1]. Abdelrhman Sayed Awad, Adil Yousif, "Enhanced Model for Cloud Data Security based on Searchable Encryption and Hybrid Fragmentation", International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)2019.

[2]. Bablu Kumar Das; Ritu Garg, "Security of Cloud Storage based on Extended Hill Cipher and Homomorphic Encryption", International Conference on Communication and Electronics Systems (ICCES)2019.

[3]. R. Nivedhaa, J.Jean Justus"A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption",International Conference on Communication and Signal Processing (ICCSP)2018.

[4]. P. Sivakumar; M. NandhaKumar, "Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud ", IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)2019.

[5]. Muthi Reddy P, S. H. Manjula "Secured Privacy Data using Multi Key Encryption in Cloud Storage", Fifth International Conference on Emerging Applications of Information Technology (EAIT)2018.

[6]. Yogita S. Gunjal ; Mahesh S. Gunjal, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing", International Conference On Advances in Communication and Computing Technology (ICACCT)2018.

[7]. Thang Hoang; Attila Altay Yavuz, “A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services”, IEEE Transactions on Services Computing (Early Access),2019.

[8]. Zhiting Zhang; Peng Zeng "Large-Universe Attribute-Based Encryption with Public Traceability for Cloud Storage",IEEE Internet of Things Journal (Early Access),2020.

[9]. Ming Zeng; Hai-Feng Qian,"Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage" IEEE ACCESS,2019.

[10]. Gongcheng Hu; Leyou Zhang,"An Expressive “Test-Decrypt-Verify” Attribute-Based Encryption Scheme with Hidden Policy for Smart Medical Cloud", IEEE Systems Journal (Early Access)2020.

[11]. Mitsuhiro Okada; Takayuki Suzuki, "FPGA-accelerated Searchable Encrypted Database Management Systems for Cloud Services",IEEE Transactions on Cloud Computing (Early Access),2020.

[12]. Yinbin Miao; Qiuyun Tong,"Verifiable Searchable Encryption Framework against Insider Keyword-Guessing Attack in Cloud Storage", IEEE Transactions on Cloud Computing (Early Access),2020.

[13]. Enrico Bacis; Sabrina De Capitani di Vimercati" Securing Resources in Decentralized Cloud Storage", IEEE Transactions on Information Forensics and Security (Volume: 15),2019.

[14]. Binanda Sengupta; Sushmita Ruj, "Efficient Proofs of Retrievability with Public Verifiability for Dynamic Cloud Storage", IEEE Transactions on Cloud Computing,2017.

[15]. Ye Tao; Peng Xu, "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage", IEEE Access,2019.

[16]. Peiyi Han; Chuanyi Liu,"CloudDLP: Transparent and Scalable Data Sanitization for Browser-Based Cloud Storage", IEEE Access ,2020.

[17]. Vikas Chouhan; Sateesh K. Peddoju,"Building a cloud-based energy storage system through digital transformation of distributed backup battery in mobile base stations" IEEE Access,2020.

[18]. Sheng Cao; Xiaosong Zhang "Toward Secure Storage in Cloud-based eHealth Systems: A Blockchain-Assisted Approach", IEEE Network (Volume: 34, Issue: 2, March/April 2020).

[19]. VIKAS CHOUHAN, SATEESH K. PEDDOJU "Investigation of Optimal Data Encoding Parameters Based on User Preference for Cloud Storage", IEEE Access (Volume: 8)2019.

[20]. Longxia Huang; Gongxuan Zhang; "A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems", IEEE Access (Volume: 8),2020.