*International Journal of Research in Advent Technology, Vol.7, No.5, May 2019*
*E-ISSN: 2321-9637*
*Available online at www.ijrat.org*

# Security Issues of Cloud Computing – A Survey

M. Suresh Kumar[1], Prof. V. Nagalakshmi[2]
*Department of Computer Science[1, 2], GITAM Institute of Science, GITAM(Deemed to be University)[1,2]*
*Email: sureshkumar.maddila@gitam.edu[1], nagalakshmi.vadlamani@gmail.com[2]*

**Abstract-** Cloud computing has been popular in the information technology architecture because cloud service providers offers many services based on user's need. Cloud storage services are the services which can provide a huge storage space to solve the bottleneck of the storage space of local end users. However, cloud storage service should have data security because the user's data is not stored at their storage area. Several cloud storage systems exist today, but most of them do not provide security guarantee in their Service Level Agreements. This lack of security support has been a major hurdle for the adoption of cloud services, especially for enterprises and cautious consumers. In this survey, recent developments, various security issues and challenges are discussed which are associated with cloud computing environment, this survey describes various existing solutions provided for dealing with security threats and will provide a comparative analysis of these approaches. This will provide better understanding of the various security problems associated with the cloud, current solution space and further research scope to deal with such problems in a better way.

**Index Terms**- Cloud computing, cloud storage, cloud service providers, data security, service level agreements.

## 1. INTRODUCTION

Cloud Computing has recently emerged as a new paradigm for hosting and delivering services over the internet. The cloud computing is an internet based environment that allows us to use software, data and services over the internet from any location on any web enabled device [1]. Nowadays, online cloud services are widely used for providing a large volume of storage space and high-end computing platforms. Hence, there is a need for providing security and integrity in the cloud resources [2]. In general, cloud infrastructures are much reliable and powerful than traditional computing platforms. However, unauthorized access and malicious users have found to be a significant issue in securing the cloud infrastructures. These unwanted users may modify or delete the information being stored in the cloud infrastructure [3, 4]. Nowadays, wide range of availability and reliability mechanisms are incorporated into the online cloud services for providing the integrity and security in cloud resources [5, 6]. In addition, on demand cloud services are provided for users over the internet.

Cloud storage service is the most common and popular service among many cloud services (Google Drive, Microsoft OneDrive, Dropbox). Users have a bottleneck in local storage space because there are many users to save data in cloud storage, so cloud storage service has high capacity which solves user's difficult problems [7]. Cloud storage service provides high capacity space, and in order to achieve ubiquitous service, it also provides to access cloud services from web service or applications that utilize the application programming interface (API) by mobile devices. Although cloud storage service has many advantages, it brings a lot of challenging issues which include efficiency and security [8]. One of the biggest challenges is verifying the integrity of the data because users cannot know how the cloud storage service handles their data. These cloud storage services are provided by commercial enterprises, so it cannot be fully trusted by the users. Therefore, the cloud service provider may hide data loss and data errors in the service to show their benefits. It is very serious when a user stores data in untrusted cloud storage, for example, a large size of the outsourced data and the client's limited resource capability and the client to find an efficient way to achieve integrity verifications without the local copy of data files [9, 10]. This paper presents an overview of the research on security of data in cloud computing environments. The characteristics of cloud computing are discussed, the methodologies used to secure sensitive data are highlighted. The performance evaluation such as storage cost, computation costs are studied to validate the efficiency of the techniques. The existing techniques are reviewed with the advantages and the limitations are highlighted.

The rest of this paper is organized as follows. Section 2 gives an overview of the characteristics of cloud computing. Section 3 describes the security issues that are needed to be solved in order to provide secure data management for cloud environments. Section 4 reviews the existing security solutions that are being used in the area of cloud computing. Section 5 describes the survey on the existing techniques for securing the sensitive data. Finally in section 6 the conclusion is made with future work.

## 2. CHARACTERISTICS OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) cloud computing reference architecture defines five major actors in the cloud such as cloud consumers, cloud providers, cloud carriers, cloud auditors and cloud brokers. Each of these actors is an entity (either a person or an organization) that participates in a cloud computing transaction or process, and/or performs cloud computing tasks. A cloud consumer is a person or organization that uses services from cloud computing tasks. A cloud provider is an entity that makes cloud services available to interested users. The activities of cloud providers can be divided into five main categories: service deployment, resource abstraction, physical resources, service management, security and privacy. A cloud auditor conducts independent assessments of cloud services, operations performance and security relation to the cloud deployment. A cloud broker is an entity that manages the use, performance and delivery of cloud services and also establishes relationships between cloud providers and cloud customers. A cloud carrier is an entity that provides connectivity and transport of cloud services from cloud providers to cloud consumers through the physical networks.

When considering cloud computing, the types of services that are offered, the way those services are delivered to those using the services and the different types of people and groups that are involved with cloud services. Cloud computing delivers computing software, platforms and infrastructures as services based on pay-as-you go models. Cloud service models can be deployed for on-demand storage and computing power in various ways: Software-as-a-Service (SaaS), Platform-as-a-Service (Paas) and Infrastrucutre–as-a-Service (Iaas). Cloud computing service models have been evolved during the past few years within a variety of domains using the "as-a-Service" concept of Cloud Computing such as Business Integration-as-a-Service, Cloud-Based Analytics-as-a-Service (CLAaaS), Data-as-a-Service (DaaS) [11]. The following table describes the feature of security that are necessary for the activities of cloud providers.

Table 1. Security Features:

| Security Context | Description |
|---|---|
| Authentication and Authorization | Authentication and authorization of cloud consumers using predefined identification schemes |
| Identity and Access Management | Cloud consumer provisioning and de provisioning via heterogeneous cloud service providers |
| Confidentiality, Integrity, Availability | Assuring the confidentiality of the data objects, authorizing data modifications and ensuring that resources are available when needed |
| Monitoring and Incident Response | Continuous monitoring of the cloud infrastructure to assure compliance with consumer security policies and auditing requirements |
| Policy Management | Defining and enforcing rules for certain actions such as auditing or proof of experience |

## 3. ISSUES OF SECURITY IN CLOUD

Cloud computing has raised several security threats such as data breaches, data loss, denial of service and malicious insiders that have been extensively studied. These threats mainly originate from issues such as multi-tenancy, loss of control over data and trust. Consequently the majority of cloud providers such as Amazon's Simple Storage Service (S3), the Google Compute Engine and the Citrix Cloud Platform which do not guarantee specific levels of security and privacy in their SLAs as part of the contractual terms and conditions between cloud providers and consumers. The major threats of cloud computing can be described as follows:

### 3.1 Multi-tenancy

Multi-tenancy refers to sharing physical devices and virtualized resources between multiple independent users. Using this kind of arrangement means that an attacker could be on the same physical machine as the target. Cloud providers use multi-tenancy features to build infrastructures that can efficiently scale to meet customer's needs, however the sharing of resources means that it can be easier for an attacker to gain access to the target data.

### 3.2 Loss of Control

Loss of control is another potential breach of security that can occur where consumer's data, applications and resources are hosted at the cloud providers owned premises. As the users do not have explicit control over their data, this makes it possible for cloud providers to perform data mining over the user's data, which can lead to security issues. In addition, when the cloud providers backup data at different data centers, the consumers cannot be sure that their data is completely erased everywhere when they delete their data. This has the potential to lead to misuse of the unerased data. In these types of situations where the consumers lose control over their data, they see the cloud provider as a black-box where they cannot directly monitor the resources transparently.

### 3.3 Trust Chain in Clouds

Trust plays an important role in attracting more consumers by assuring on cloud providers. Due to loss of control, cloud users rely on the cloud providers using trust mechanisms as an alternative to giving users transparent control over their data and cloud resources. Therefore cloud providers build confidence amongst their customers by assuring them that the provider's operations are certified in compliance with organizational safeguards and standards.

## 4. SYSTEM MODEL

A representative network architecture for cloud data storage is illustrated I Fig 1. Three different network entities can be identified as follows:

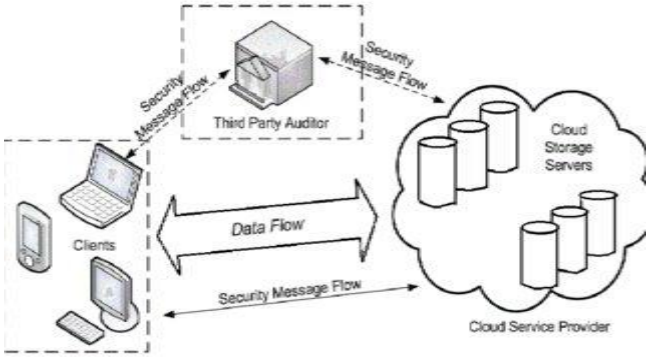


Fig 1: System Architecture [12]

- Client an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.
- Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the client's data.
- Third Party Author (TPA): an entity, which has expertise and capabilities that clients do not have, is trusted to access and expose risk of cloud storage services on behalf of the clients upon request.

In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies. In case, the clients do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA. To secure the data effectively, the methodologies are described in the next section.

### 4.1 Methodology

There are several techniques used to secure the user's data while storing in cloud computing. In general, the verification schemes are classified into two types, namely, probabilistic and deterministic. Deterministic methods are more costly than the probabilistic method. The vital role of the deterministic methods is for examining the remotely stored data. The probabilistic methods focus on random verification of outsourced data [13]. The deterministic methods verify the data in the data warehouse. In this section, the review of the four techniques such as Encryption, Encoding, Steganography and Nth Order Binary Encoding (NOBE) are described in detail.

#### 4.1.1 Encryption

In general, a data encryption method uses statistical methods and probabilistic models to convert the plain text into ciphertext. This ciphertext is not possible by a user to read and understand. The authorized users have a key to decrypt the ciphertext into the original version plain text. Nowadays, a web browser automatically encrypts the client request into ciphertext. Hence, the unauthorized users or malicious user are protected from accessing the confidential data. Though, a malicious user or unauthorized user can capture the encrypted data, they cannot understand the original information. The data encryption methods are classified into symmetric and asymmetric based data encryption algorithms. In the early days, 64-bit encryption methods, 128-bit encryption methods were used. Later, Advanced Encryption Standard (AES), DES and Blowfish which come under the method of symmetric key algorithms were used. RSA and Diffie-Hellman key exchange methods come under asymmetric key encryption methods.

#### 4.1.2 Encoding

The encoding schemes are used for changing the original data into a different format that can be accessed only by the authorized user. The American Standard Code for Information Interchange (ASCII) is widely used for encoding the data. The ASCII consists of a range of non-printable and printable methods that classify the lowercase and uppercase letters, punctuation, marks, symbols and numbers. In some cases, an exclusive number is used for encoding the input data. In general, zero to 127 characters are found to be a standard ASCII. Moreover, 128-255 characters are considered as undefined values. Recently, the BinHex, Uuencode and MIME are also used to encode the data. Moreover, the encoding methods are also used for reducing the size of audio and video files. An appropriate coder-decoder is used during the encoding process of audio and video files. Nowadays, encoding methods are widely used for encoding the secure data stored in cloud storage.

#### 4.1.3 Steganography

Nowadays, users send the data to the receiver with encryption techniques. In some cases, the organizations are not allowed to use any encrypted emails and communication. This would increase the access of the malicious user and unauthorized access. To overcome this issue, a variety of steganography methods are introduced in recent years. The steganography methods are used to communicate the data between the sender and receiver where the data communication is not understood by third parties. In this method, secret data is covered with the help of various types of images, audio, and video. Nowadays, cloud computing users have started using of steganography methods for secure communication between the sender and receiver. In general the hidden information using steganography methods are stored in the least significant bits of a digitized file. This technique is not possible to read by the human eye. However, an authorized user can use a proper steganography method to understand the meaning of the hidden data.

4.1.4 Nth Order Binary Encoding (NOBE)

NOBE based data compression technique is found to be a significant technique than the existing data compression methods. As a compression ratio for the NOBE based data compression technique is very high, it is widely used for securing the cloud resources effectively. By using different techniques to secure the user's data, some security evaluation goal can be achieved. This can be described in below section.

### 4.2 Goal for Security Evaluation

There are five goals for security evaluation in cloud computing such as dynamic data, batch auditing, blockless verification, stateless verification and privacy preserving.
Blockless Verification: The auditor can verify data blocks and need not retrieve all audited data blocks in the cloud storage service. Stateless verification is that the auditor need not maintain and update data situation because data situation is maintained by the client and cloud storage service together.
Batch Auditing: The auditor can verify the data of different clients at the same time because the auditor can be delegated by lot of clients.
Dynamic Data: The data owner can insert, modify and delete blocks in the cloud storage service because their data can be continuously updated at any time.
Privacy Preserving: The auditor can get knowledge which is delegated data from the response of the cloud storage service. The several parameters that are used to validate the performance of techniques are represented in the below section.

### 4.3 Performance Evaluation

The methods for secure data storage are evaluated in terms of two factors such as the security properties that each scheme provides and the system cost on a CSP and a client Regarding the security threats presented in Section 3. A method is required to satisfy the following security properties [23]:
Confidentiality: The original data content outsourced to cloud storage should not be revealed to anyone except the user who owns the data.
Availability: The outsourced data should always be available to users who own the data, even during system failure.
Data integrity: A client or CSP should be able to verify that whether the outsourced data has not been modified or deleted.
Computing Cost: In order to achieve an efficient auditing, the method will analyze the client. TPA and cloud storage service cost on the computing resources.
Storage Cost: Because the client will upload data to the cloud storage service without the local copy of data files, the method will analyze the client, TPA and cloud storage service cost on the storage spaces.

## 5. LITERATURE REVIEW

Several techniques are suggested by researchers in the security of cloud computing architecture. In this scenario, brief evaluations of some important contributions to the existing techniques are presented.

Contribution of existing techniques:

Author: Baojiang Cui, et al.,(2016) [14]
Methodology Employed: Developed a Key Aggregate Searchable Encryption (KASE) to address the problem of secure communication storage and complexity.
Motivation: The method uses the searchable key encryption technique for preserving privacy of user's data.
Advantage: To share large number of documents, data owner distribute a single key to user and a single trapdoor is enough for querying the shared documents.
Limitation: The user shares a query document to multiple owners only by generating multiple trapdoors to the cloud. The KASE model provides poor performance in federated clouds.
Performance Measure: The performance of KASE can be evaluated by cost of time to encrypt, decrypt, adjust, keyword search, trapdoor and test.

Author: V. R. Pancholi and B. P. Patel, (2016) [15]
Methodology Employed: Designed AES to secure the data.
Motivation: This method chooses symmetric cryptosystem because it has the speed and computational efficiency to handle encryption of large volumes of data.

Advantage: In AES, data was protected against future attacks such as smash attacks. AES encryption algorithm had a minimal storage space and high performance without any weaknesses and limitations.
Limitation: But, the running time of AES algorithm was high because the 128 bits were interpreted as 16 bytes and again start the algorithm to get the ciphertext as output
Performance Measure: Encryption time and decryption time.

Author: Y. Yu et al., (2017) [16]
Methodology Employed: Designed an Identity-based (ID-based) remote data integrity checking (RDIC) protocol to reduce the system complexity and the cost for managing the public key authentication framework.
Motivation: The method uses the key-homomorphic cryptographic primitive in public key infrastructure (PKI) based RDIC schemes to preserve the privacy of user's data.
Advantage: The proposed ID-based RDIC protocol leaks no information of the stored data to the verifier during the RDIC process. The new construction is proven secure against the malicious server in the genetic group model and achieves zero knowledge privacy against a verifier.
Limitation: The cost of implementation is too expensive than the other existing techniques.
Performance Measure: The performance of ID-based RDIC was validated by using metrics such as computation cost, communication cost and storage cost.

Author: Y. Li et al., (2017) [17]
Methodology Employed: Developed a Security-Aware Efficient Distributed Storage (SA-EDS) model, Alternative Data Distribution (AD2) Algorithm, Secure Efficient Data Distributions (SED2) Algorithm and Efficient Data Conflation (EDCon) Algorithm to increase the adoptability of cloud computing.
Motivation: This research paper focuses on the issue of user's anxiety and proposes an intelligent cryptography approach, by which the cloud service operators cannot directly reach partial data.
Advantage: The proposed approach divides the file and separately stores the data in the distributed cloud servers. An SED2 approach was designed to determine whether the data packets need a split in order to shorten the operation time.
Limitation: There is no data availability feature which causes failure of data retrievals due to data center's down.
Performance Measure: In order to evaluate the performance of SA-EDS, its execution time was used while different input data sizes were operated.

Author: C. Wang et al., (2013) [18]
Methodology Employed: Proposed a privacy-preserving public auditing system for data storage security in cloud computing. This method utilized the homomorphic linear authenticator and random masking to guarantee that the Third Party Author (TPA) would not gain any knowledge about the data stored.
Motivation: By using this auditing scheme, the users stored their data with high data integrity protection without the burden of local storage and maintenance.
Advantage: During the efficient auditing process, the method eliminates the burden of cloud users from the tedious possibly expensive auditing task and also alleviates the user's fear of their outsourced data leakage.
Limitation: TPA cannot audit for multiple users but handle multiple audit sessions from different users for their outsourced data files.
Performance Measure: Cost of Privacy-Preserving Protocol Batch Auditing Efficiency. Sorting out invalid response are the metrics used to evaluate the performance of auditing method.

Author: J K Liu et al., (2016) [19]
Methodology Employed: Proposed a two factor data security protection mechanism with factor revocability for cloud storage system.
Motivation: The process of sending data to use is completely transparent in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both secret key and a security device to gain access to the data.
Advantage: The method enhanced the confidentiality of the data and also offers the revocability of the device so that once the device is revoked the corresponding ciphertext will be updated automatically by the cloud server without any notice of the data owner.
Limitation: The running time of the system was high in device generation and updation. Even though the method achieved a two factor protection, it faced the additional complexity which degrades the systems performance.
Performance Measure: The experiments analyzed the efficiency of this mechanism in terms of computational and communicational cost.

Author: Y. Ren, et al., (2016) [20]
Methodology Employed: Develop the highly efficient data integrity scheme for cloud storage for mobile health applications.
Motivation: The method overcomes the limitations of TPA proofs of storage (POS) schemes which employ expensive operations to generate authentication tags and check the tags for data blocks. Such heavy computation demand is not appropriate for biosensor nodes.
Advantage: The authentication tag for each data block generated by biosensor node is minimal in this scheme due to the use of hash operation. In data integrity checking phase, message-locked encryption scheme is utilized to

encrypt and transport the auditing information of the checked data blocks, which significantly reduces the required amount of calculation and communication resources.
Limitation: The method used the de-duplication cloud storage platform to reduce the burden of storage system, but did not focus on the security for de-duplication data. The duplication data can be accessed by unauthorized users in the cloud.
Performance Measure: The performance metrics such as throughput of tag preprocessing, communication cost, computation cost and storage cost to validate the performance of data integrity method.
Author: K. Fan, et al., (2018) [21]
Methodology Employed: Developed the public auditing scheme as Dynamic Index Table (DIT) to support the dynamic operations stored by users.
Motivation: The DIT method focused on reply attack by using remote data auditing in cloud storage. Also allows the user to store the data structure locally for dynamic operations.
Advantage: The DIT method avoids the TPA to know more information about outsourced data. During dynamic process, DIT reduced the computation cost of users based on Merkle Hash Tree (MHT).
Limitation: The modification time of MHT is longer because it uses only one signature calculation to compute two data block signature.
Performance Measure: The communication cost and computation costs are used to validate the effectiveness of DIT.

Author: K. Loheshwaran, and J. Premalatha, (2016) [22]
Methodology Employed: To secure the data in cloud storage, a renaissance system model is proposed.
Motivation: The method secures the data by using code regeneration, the dat integrity checking and renewal are implemented by TPA and a proxy separately on behalf of the data owner.
Advantage: The proposed model is a semi trusted proxy agent that performs instead of the data owner in order to reinstate the data blocks that are obtained during the repair process.
Limitation: The system delay is caused by the security overhead both in the cloud user's side that is while generating the signature and symmetric encryption.
Performance Measure: Traffic Load Response rate, average utilization computation and average net profit are used as performance metrics.

## 6. CONCLUSION

The evolution of cloud computing made a major change in the computing world as with the assistance of the basic cloud computing service models such as SaaS, PaaS and IaaS. An organization achieves their business goals with minimum effort as compared to the traditional computing environment. On the other hand, security of the data in the cloud database server is the key area of concern in the acceptance of the cloud. This paper is a survey about the recent advances in security and also discusses different security challenges in the area of cloud computing. Security factors that affect the activities of cloud providers in relation to the legal processioning of consumer data were identified and a review of existing research was done to summarize the state-of-the-art field. For future development, data security will be more difficult with the generation of big data. This is so because big data has three characteristics which include volume, velocity and variety which can affect the implementation of data verification.

**Acknowledgments**

We are very much thankful to all the researchers and the web resources for sharing their work and knowledge. Our sincere acknowledgements to all who made this work possible.

## REFERENCES

[1] K. B. Deepaklal, "Fuzzy Keywoard Search over Encrypted Data in Multicloud", Discovery, Volume 3, Issue 1, January – February 2014.
[2] Wang C, Wang Q, Ren K, Cao N, Lou W.(2012). "Toward Secure and Dependable Storage Services in Cloud Computing". IEEE Transactions on Services Computing. 5(2), 220-232.
[3] Bharat B. Madan, Manoj Banik, Bo Chen Wu, Doina Bein, "Intrusion Tolerant Multi-Cloud Distributed Storage", IEEE International Conference on Smart Cloud, IEEE, 2016, 262-268.
[4] Jin Li, Yinghui Zhang, Chen X, Xiang Y, "Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing", Volume 72, Computers and Security, Jan 2018, 1-12.
[5] Qi Jiang, Jianfeng Ma, Fushan Wei, "On the Security of a Privacy-Aware Authentication Scheme for Distribuuted Mobile Cloud Computing Services", Volume 12, No 2, IEEE Systems Journal , June 2018, 2039-2042.
[6] B. B. Gupta, Shingo Yamaguchi, Dharma P. Agrawal, "Advances in Security and Privacy of Multimedia Big Data in Mobile and Cloud Computing", Volume 77, Issue 7, Multimedia Tools and Applications, April 2018, 9203-9208.
[7] Ping Li, Jin Li, Zhengan Huang, Chong-Zhi Gao, Wen-Bin Chen, Kai Chen, "Privacy Preserving Outsourced Classification in Cloud Computing", Volume 21, Issue 1, Cluster Computing, March 2018, 277-286.

[8] External Integrity Verification for Outsourced Big data in Cloud and IoT: A big picture, Chang Liu, Chi Yang, Xuyun Zhang, Jinjun Chen, Volume 49, Future Generation Computer Sysems, August 2015, 58-67.

[9] Kayalvizhi S, Jagadeswari S, "Data Dynamics for Storage Security and Public Audability in Cloud Computing", Journal of Computer Applications, Volume 5, Issue EICA2012, February 2012, 44-51.

[10] N. Praveen Kumarga, D. Sireesha, "Ensuring Data Integrity in Cloud Computing", International Journal of Computer Science and Network Security, Volume 14, No. 9, September 2014, 34-38.

[11] Sugam Sharma, U. Sunday Tim, Shashi K. Gadia, Johnny S. Wong, "Proliferating Cloud Density through Big Data Ecosystem, Novel XCLOUDX Classification and Emergence of as-a-Service Era", Data Science Journal, 2016, 1-20.

[12] Qian Wang, Cong wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Volume 22, No 5, May 2011, 847-859.

[13] Syam Kumar P, Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", International Journal of Computer Science Issues, Volume 8, Issue 6 No 1, November 2011, 261-274.

[14] Baojiang Cui, Zheli Liu, Lingyu Wang, "Key Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on Computers, Volume 65, No 8, August 2016, 2374-2385.

[15] Vishal R. Pancholi, Dr. Bhadresh P. Patel, "Enhancement of CC Security with Secure Data Storage using AES", International Journal for Innovative Research in Science and Technology, Volume 2, Issue 9, February 2016, 18-21.

[16] Yong Yu, Man Ho Au, G. Atenise, X. Huang, W. Susilo, Y. Dai, G. Min, "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information forensics and Security, Volume 12, No 4. April 2017, 767-778.

[17] Li Yibin, Keke Gai, Longfei Qiu, Meikang Qiu, Zhao Hui, "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing", Information Sciences, Volume 387, May 2017, 103-115.

[18] C. Wang, S. S. M. Chow, Q. Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Volume 62, No 2, 2013, 362-375.

[19] J. K. Liu, K. Liang W. Susilo, J. Liu, Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, Volume 65, No 6, June 2016, 1992-2004.

[20] Y Ren, J Shen, Y Zheng, J Wang, Han-Chieh Chao, "Efficient Data Integrity Auditing for Storage Security in Mobile Health Cloud", Peer-to-Peer Networking and Applications, Volume 9, issue 5, September 2016, 854-863.

[21] K. Fan, M. Liu, G. Dong, W. Shi, "Enhancing Cloud Storage Security Against a New replay Attack with an Efficient Public Auditing Scheme", The Journal of Supercomputing, 2018, 1-27.

[22] K. Loheswaran, J. Premalatha, "Renaissance System Model Improving Security and Third Party Auditing in Cloud Computing", Wireless Personal Communications, Volume 90, Issue 2, September 2016, 1051-1066.

[23] W Xia, H Jiang D Feng, Y Hua, "Similarity and Locality based Indexing for High Performance Data Deduplication", IEEE Transactions on Computers, Volume 64, No 4, April 2015, 1162-1176.