Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey

Jeevitha B. K.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering
Bangalore University,
Bangalore-560001

Thriveni J.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering
Bangalore University,
Bangalore-560001

Venugopal K. R.
Department of Computer Science and Engineering
University Visvesvaraya College of Engineering
Bangalore University,
Bangalore-560001

ABSTRACT
Cloud Computing is a form of distributed computing wherein resources and application platforms are distributed over the Internet through on demand and pay on utilization basis. Data Storage is main feature that cloud data centres are provided to the companies/organizations to preserve huge data. But still few organizations are not ready to use cloud technology due to lack of security. This paper describes the different techniques along with few security challenges, advantages and also disadvantages. It also provides the analysis of data security issues and privacy protection affairs related to cloud computing by preventing data access from unauthorized users, managing sensitive data, providing accuracy and consistency of data stored.

Keywords
Storage Area Network Trusted Computing Group, CeritificateLess Proxy Re- Encryption, Elliptic Curve Cryptography, Dynamic Hash Table.

1. INTRODUCTION
Cloud refers to the network that provides services to network through internet. It is a model that enables the characteristics like on demand self-service, pay-as-you-use-service. National Institute of Standards and Technology (NIST) [1] defines cloud computing as a convenient, on-demand computing resources for storage services. Deployment models define purpose, applications and access to the cloud like public, private, hybrid and community. Service models are categorized into the three models like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Cloud is an enormous shared computing resource which includes Data Storage. It is managed by a cloud service provider on cloud data servers built on virtualization techniques known as utility storage. Most of the storage clouds run on the public internet cloud by well-known companies like Amazon, Dropbox and Google. A few bigger associations have discovered esteem in running private cloud inside their own data centres.

1.1 Cloud Data Storage
Cloud storage is a utility where data is remotely maintained, managed and backed up in cloud environment and then the data is accessible to end users over internet. It permits the client to collect the files through online so that the client these files from anywhere via internet. Even though there are many advantages of cloud storage, few companies are still in dilemma to use the benefits of cloud computing technologies for not having proper security. The main objective of the cloud storage is to store the data safely in the free space and fetch the data whenever requested by the client.

Security and Privacy are the distinguished methods used to secure the information from attackers. Third party is used as service providers to grasp the data sent by owner by offline mode in cloud environment. Sometimes cloud may reveal the data by accidentally for unauthorized purpose which strikes the results of privacy and confidentiality. When there is no direct link between clients and servers, master server comes into picture. Chunking operation [2] is used for storing duplicate records to give data backup from improvements. Clients performs dynamic data operations to store data as tokens in master server and the records are filed in slave servers using token generation and merging algorithms.

Cloud storage service often provides applications, services to users to access the storage capacity. It is hosted by Storage Service Provider (SSP) [3] along with the combination of Storage Servers. This SSP is plotted on storage virtualization architecture. SSP provides, manages the storage infrastructure to store the data of third party and is arranged as an online storage service provider, virtual storage service provider or cloud storage service provider. SSP has a facility that provides large storage infrastructure i.e., Storage Area Network (SAN) and it is distributed between the users/enterprises. A SSP provides a specific storage capacity that can be scaled depending upon user requirements. It may be used for various purposes such as data backup, data recovery, sharing and collaboration of various consumer/businesses well as with other applications. Multiple-Replica Provable Data Possession (MR-PDP) [4] solves the assumption that multiple copies of data are stored instead of single copy. To overcome this assumption a protocol is used called a challenge-response protocol to verify the number of replicas of the file. MR-PDP is more efficient for storing replicas than a single replica PDP scheme. Customer driven SLA-based resource provisioning algorithms is proposed in Linlin et al., [5] to reduce cost by minimizing resource and improve CSL by reducing SLA violations.

The rest of this paper is organized as follows. Section 2 describes Cloud Storage Security and Privacy. Section 3 addresses Mobile Cloud Data Storage Security and privacy. Finally, conclusions are presented in section 4.

2. CLOUD DATA STORAGE SECURITY AND PRIVACY

Cloud Computing provides many technologies for security issues like Service Oriented Architecture (SOA), virtualization, Web 2.0 etc., [6]. Virtualization allows multiple users to share a physical server.

In virtualization environment, storage strengthening at the file system is desirable, because it enables data sharing, administration efficiency and performance optimization. Here, the security requirements in multitenant file systems are analysed first. Then the Dike authorization architecture is introduced by Kappes et al., [7], combines access control with tenant's namespace isolation that is backwards compatible to object based file systems.

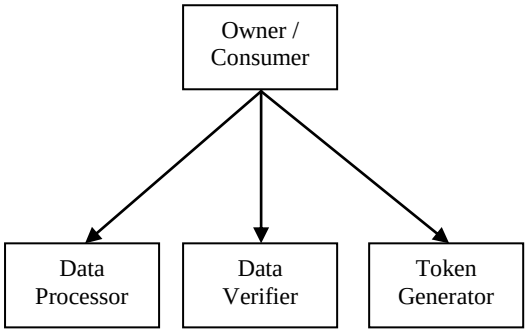

Fig 1: Architecture of Owner-Consumer Relationship

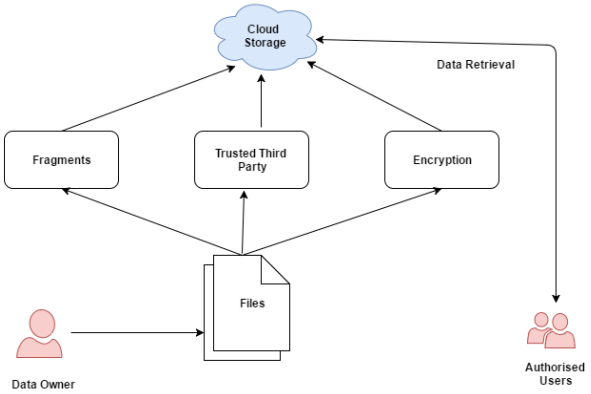

Fig 2: The Architecture of Data Storing Security and Privacy.

Chintada et al., [8] classifies the security affairs related to Cloud Computing is broadly into two categories, i.e., Security issues accepted by cloud providers and the cloud customers. The Cloud provider must protect their infrastructure, so that the client's information and applications are secured while the customer must satisfy the provider's infrastructure is secured completely to secure the customers information.

High Availability and Integrity Layer (HAIL) [9] model helps in developing a tool to improve the security and efficiency. HAIL helps in managing the file integrity and helps in availability of file across the set of servers or independent storage device. HAIL offers some benefits like Strong file intactness assurance, Low overhead, Strong adversarial model, direct client-server communication and Static/dynamic file protection. Spillner [10] explores the life-cycle of consumer by accomplishing the storage service by optimality with resource provider. An architecture has been proposed which contains three components i.e., data processor that processes data before it is sent to the cloud, data verifier that checks whether the data in cloud has been tampered and token generator that generates the token which helps the storage provider to retrieve segments of consumer data as shown in Fig. 1 [11].

Victor [12] developed a Cloud Computing Adoption Framework (CCAF) to secure the stored data in multi-layered (Three Layer) cloud: Firewall and Access control; Identity Management and Intrusion Prevention and Convergent Encryption. The Architecture of data storage security and privacy is showed in figure 2.

2.1 Data Security

Data security has become a major problem in IT because of the data to be stored securely in servers. From the perspective of data security, Cloud Computing creates new challenges on security threats for many reasons like external data storage, multi-tenancy, dependency on internet, lack of control over data and also internal security. Traditional algorithms will not be having control over the data that is accepted by the cloud [13] [14] [15].

Cloud computing shifts the data, software and databases to the large data centres (server farms) in which repository is used to store, manage and dissemination of the data. T Boneh et al., [16] use digital signature for fine-grained control over user's security privileges. Raghavendra et al., [17] proposes an efficient approach for keyword search to achieve security on outsourced data by involving index generation method along with splitting method for keyword splitting. These keywords are stored using wildcard based techniques that are stored securely with low cost for storage.

In general, traditional symmetric encryption algorithms, such as DES and AES provide relatively lower security and encrypted data are vulnerable to attacks. Danwei et al. [18] propose a strategy to secure data by splitting the data into sections by using data splitting algorithm which assures data reliability. Prakar and Kak [19] splits the stored data and are stored at distinct places on the network and these pieces are backed up in a single server. Sometimes the clients forget the password that are assigned and these leads to brute force attacks. Mazhar Ali et al., [20] also splits the data in the DROPS methodology into number of fragments which are distributed to multiple nodes. These nodes are separated using T-colouring. The fragmentation and distribution ensures that no single node reveals the information to attackers. The performance and security of the DROPS methodology analysed in terms of retrieval time.

Nayak et al., [21] checks the honesty of the service provider by using data reading protocol. After verifying the honesty of the data stored, a system structure has been designed with three data backups for rehabilitation of data. These backups are residing in different places of primary server. This structure uses SHA Hash algorithm for encryption, SFSPL algorithm for splitting files and GZIP algorithm for compressing the data.

Hiremath et al., [22] first presents the network architecture to deploy and evaluating secure data storage issues and then desired properties of public auditing services which are depended on cloud data storage are encouraged systematically and cryptographically. Patel and Dansena [23] have implemented Trusted Platform Module (TPM) to compute the Trusted Computing Group (TCG) [24]. TPM is also used to generate the keys to decrypt the data.

2.1.1 Data Access

Data access refers to a user's ability to access or retrieve data that is stored within a database or other repository. Xu et al., [25] developed CeritificateLess Proxy Re- Encryption (CL-PRE), a new proxy-based re-encryption scheme augmented with certificateless public key cryptography. CL-PRE is used for data storage and also to generate secret key and distributed to users for securely sharing the data. Along with CL-PRE, symmetric data encryption is used for encryption purpose by generating proxy re-encryption keys. The data is decrypted using by using users private key. uses MCL-PKE and Security Mediator (SEM) to get the key that is used to get back partial private key information.

Kaitai and Willy [26] proposed a searchable attribute-based re-encryption system that supports primitives like abilities and flexible keyword update service. This scheme uses a sharing policy in which the data owner shares the data to a specified group of users efficiently that matches to the policy. A separate search keyword is maintained and updated after sharing the data. Bala Chandran et al., [27] propose a new model through distributed auditing mechanism to assure the data correction of the data stored. Neha and Ganeshan [28] use Elliptic Curve Cryptography (ECC) for encryption purpose and connection is established using Diffie-Hellman key exchange mechanism in order to achieve data integrity, reduce loss of data and also securely access the data [29].

Mokhtarnameh [30] proposed a key generation technique for certificateless public key cryptography in order to have one public key for one private key. By using CL-PRE, Bilinear Diffie-Hellman problem is solved. Jianghong et al., [31] propose a revocable-storage identity-based encryption (RS-IBE) [32], which introduces the operations of user revocation and updating of ciphertext to provide the forward/backward security. Hou et al., [33] use the traditional ID-based public key (IPK) cryptosystem and traditional IPK to achieve an efficient two party authenticated key agreement protocol based on certificateless public key encryption scheme. It achieves both forward and backward secrecy. Melissa [34] uses multi-authority scheme which identify the attributes by each user. Identify Based Encryption (IBE) is used to focus on the abilities of decryption of ciphertext. Yinxia Sun and Futai Zhang [35] uses Identity-based Cryptography (ID-PKC) which eliminates the need for certificate by deriving public keys for users directly from their human-memorizable information, such as e-mail address and IP address. The private keys are fully generated by a Private Key Generator (PKG) which inevitably introduces the key escrow problem.

Deepa et al. [36] prevents accessing the data from unauthorized users by proposing a homomorphism based token system to verify the erasure-coded data. Zebin et al., [37] discusses the possibility of exploiting cloud computing architectures for parallel and distributed dimensionality reduction and storing of remotely sensed hyper spectral datasets in large data repositories and presents a cloud computing implementation of the PCA algorithm on Spark platform.

Yang [38] proposes a data access control for Multi-authority cloud storage (DAC-MACS) schemes, a secure data CP-ABE method that was proposed with attribute revocation method to attain both forward and backward security [39]. Bottleneck Problem can be controlled by inter-connecting components of cloud via peer-to-peer routing and also identifies single point failure.

Bremer [41], Heng [42], Garcia [43] and Kavalionak [44] all four authors combine peer-to-peer computing and cloud computing. Bermer [41] combines the p2p and cloud that is able to self -regulate the amount of cloud resources when peer resources are not enough and it includes backup, storage, streaming, content distribution and online gaming. Heng et al., [42] combines both cloud and p2p computing to offer highly available storage service. Garcia [43] design a p2p Cloud model which gives storage service that provides computing power and flexibility to customers that provide advantages like scalability, confidentiality, file sharing, data replication and data management, quality of service, decentralization and transparency. Kavalionak [44] combines cloud and p2p to achieve a peer-assisted cloud that makes a symbiotic coupling between cloud and p2p that maintains most of the quality of service properties of the cloud and makes use of p2p functionality to reduce the operational cost.

Babaoglu et al., [45] designs a p2p cloud system (P2PCS) that makes use of gossip-based protocol to manage a large unreliable resources pool without any central co-ordinator. Li [46] makes use of ERC in p2p storage that greatly improves data reliability and reduce backup server cost. Reed-Solomom (RS) code is much suited for p2p storage cloud. Sanghamitra et al., [47] use the existing goal based threat modelling approach that enables threat modelling for developing designs for secure systems. Countermeasures of P2P cloud has been modelled using threat-SIG. Ranjan et al., [48] uses the cloud peer that generates VMs network to supporting scalable, selfless service and also load balancing.

Azad and Aftab [49] mainly concentrate on newness in the data after updating, trust between third party, CSP and also authorized user. Authorized users do not have the permission to access the stored data but also can be updated. After updating, only the authorized users can access the updated data but not the revoked users. Revoked users cannot see the updated data; they can access the previous data before updation. Trusted Third Party (TTP) is used to determine the dishonest party. Xue and Hong [50] proposes proxy framework that uses proxy signature schemes to securely share the data. Digital envelopes are used to secure the session keys. TGDH scheme is used to update key pair whenever members leave or joined the group. Proxy re-encryption [51]-[54] is used to provide forward secrecy and backward secrecy to reduce the computational overheads.

Internet of Things (IoT) is a platform that anyone can transfer data over a network without any interaction. While storing the data, organizations have options to store on cloud. To achieve this, Jayanth [55] uses role based access policies to provide secure data storage in the cloud enforcing cryptographic technique. Zhou et al. Jiang et al., [56] proposes a data storage framework for storing massive data storage of IoT by combining both structured and unstructured data. This framework combines different databases and Hadoop is used to store and manage different types of data collected by sensors and RFID readers. The different data access techniques are dicussed in Table 1.

2.1.2 Data Confidentiality

Data confidentiality is attained by encrypting the data. The dependency on cloud data storage increases the interest in security is also involved in data confidentiality even after deletion of data. As the data is stored in different places (means different copies) in order to maintain reliability, some data may remain even though a user deletes that data.

Tang et al., [57] propose File Assured Deletion (FADE) is an ideal key management system [58] in which there is a secure channel is established between cloud-client and also between client managers; the client generates key for data encryption and virtually stores with key manager and forgets the keys. This leads to neglecting communication security and impacts on cloud storage security. Habib et al., [59] propose Simplified File Assured Deletion (SFADE) that removes completely the dependency on key managed system and also assures the deletion of data of the owner to maintain data confidentiality. Users do not trust the cloud service providers (CSPs) and it is difficult to provide data security. Hence it is critical to develop efficient auditing techniques to data owners trust and confidence in storing the data in cloud. Hui et al., [60] proposes a public auditing scheme combined with Dynamic Hash Table (DHT) for securing the data. Homomorphic authenticator along with random masking based public key to achieve privacy. An entropy based algorithm is deployed on federated clouds by Wen et al., [61] to deploy the workflow application, then Bell-Lapadula Multi-level security model is used to address the security measures. The different techniques of data confidentiality are discussed in Table 2.

Table 1. Comparison of Different Data Access Techniques

Author	Algorithm	Performance	Advantages	Disadvantages
Mazar Ali et al., 2015 [20]	Fragment placement, Fragement replication	Improves Retrieval Time.	Full data is not revealed on attack of single node.	Time and Resource consumption is more.
Kaitai et al., 2015 [27]	Searchable Attribute based proxy reencryption system	The system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy.	Secure ciphertext	
Peng et al., 2016 [33]	Conditional Identitybased Broadcast PRE (CIBPRE)	CIBPRE allows a sender to encrypt a message by identifying the receivers identity.	Efficient in respect to communication.	
Mazhar Ali et al., 2015 [55]	DaSCE and Shamirs scheme	DaSCE was evaluated based on the time consumption during file upload and download.	DaSCE provides high security standards and does not compromise the keys under outsourced data.	DaSCE methodology can be extended to secure group shared data and secure data forwarding.

Table 2. Comparison of Different Data Confidentiality Techniques

Author	Algorithm	Performance	Advantages	Disadvantages
Durga et al., [61] 2016	Public Auditing Scheme, Dynamic Hash Table	New two-dimensional data structure used to verify the data property information for dynamic auditing.	Reduces the computational cost and communication overhead.	Scheme further exploits the aggregate BLS signature technique from bilinear maps to perform multiple auditing tasks simultaneously.
Zhenyu et al., [62] 2014	Entropy based algorithm, Bell-Lapadula model	Deployment of workflow application on federated Clouds.	More secure and less expensive.	Computation Overhead.
Zhongyuan et al., [78] 2016	Cluster Content Caching	Improve data availability by combining centralized clouds with client-side storage system.	Highly available and durable system with lower costs.	

Table 3. Comparison of Different Data Integrity Techniques.

Author	Algorithm	Performance	Advantages	Disadvantages
Zhongyuan et al., [64] 2016	Cluster Content Caching structure in C-RANS	By using a stochastic geometry-based network model, the effective capacity can be achieved	Effective capacity and energy efficiency	Performance is improved by combining the designs of RRU allocation and RRH association
Shubhashis et al., [69] 2015	Data Vaporizer	Advanced techniques of secret sharing of the keys to improve the security level and reliability	Storage cost is minimum	Design of highly configurable framework for data storage on top of cheap commodity cloud storage
Yong et al., [72] 2016	Public integrity auditing scheme	A cloud server can collude with a revoked user to deceive a third-party auditor (TPA) that a stored file keeps virgin even when the entire file has been deleted	Achieve the basic property of a secure auditing scheme soundness	Aforementioned attacks
Huagun et al., [74] 2016	ID-PUIC	Realizes checking of data integrity of both private/public authorization	Checking of the integrity on clouds improve the performance	Computation overhead is more

2.2.3 Data Integrity

Data Integrity is a basic component of security. It refers to the correctness and consistency of stored data in a database. Managing integrity of data is an important issue. Third Party Auditor (TPA) eliminates the involvement of client and Public Verifiability to check the integrity of data. Proof of Retrievability model is improved by deploying the Merkle Hash Tree (MHT) [62] [63] for the construction of block tag for authentication purpose.

Wang et al., [64] describes a mechanism to securely share the data efficiently with others by using the aggregate key in the cloud. To support cloud data storage, combined compressed secret keys are used in public-key cryptosystems which is more flexible than hierarchical key assignment. Dong et al., [65] propose a strategy know as Intermediate Data Dependency Graph (IDG) which discusses about the data which is generated after execution and to store these intermediate data at minimum cost. Because of fixed nature of the location, IDG is not applicable to distributed application. Sengupta et al., [66] propose Data Vaporizer (DV) that stores the data in multiple clouds or storage zones to maintain data integrity and confidentiality. Advanced techniques ig secret key sharing is considered to control fault-tolerance and also to improve the security from attackers.

Saxena and Dey [67] refer the Cloud Audit to provide a better and efficient data integrity verification technique that gives Data as a Service (DaaS). It uses a Homomorphic cryptography system with homormorphic tag that tags a special distinct verifiable value to each data block, which results in releasing data operation on each block. Leena et al., [68] combines the GIS software and also the cloud services to make Cloud GIS to complete Decision Support System (DSS) which enhances the data integrity verification and accuracy information related to agriculture stored in cloud.

Wang et al., [69] proposes ID-PUIC in public cloud and also different aspects of integrity checking like private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the authorization. The different data integrity techniques are showed in Table 3.

2.1.3 Data Availability

Mingqiang et al., [70] built a CDstore a unified multi-cloud storage solution for clients to outsource backup data with reliability and security. CDStore also adopts two-stage deduplication to attain bandwidth and to prevent channel attacks. Seungyeop et al., [71] designed, implemented and evaluated MetaSync, a file synchronization service for multiple cloud. Paxos is also implemented to provide the consistency that enables the efficiency of unchanged APIs. It provides better availability and confidentiality. Yang et al., [72] and Zhongyuan et al., [73] show the need to advance the data availability by amplifying the centralized clouds by compressing the costs to achieve the efficient storage system. The servers in data centre and peers at the network edge added each other resulting in high availability and durable system with lower costs. As the need for cloud storage system shows its growth exponentially, Data deduplication can effectively shorten the size of data by eliminating unnecessary data in storage systems.

Table 4. Comparison of Different Data Availability Techniques

Author	Algorithm	Performance	Advantages	Disadvantages
Zhang et al., [81] 2015	CHARM	Integrates two key functions 1. selecting suitable clouds 2. Transition process to redistribute data	Saves cost	
Xu et al., [79] 2015	DelayDedupe	Delaydedupe is combined with replica management that determines new duplicated chunks	Reduces response time	
Mingqiang et al., [75] 2016	CDstore	A unified multi-cloud storage solution for users to outsource backup data	Guarantees reliability, security and cost efficient	
Seungycon et al., [76] 2016	MetaSync	Provides multiple cloud synchronization services as untrusted storage providers	Provides better availability, stronger confidentiality and integrity	

Xu and Tu [74] proposed a delayed target-deduplication scheme based on the chunk-level deduplication and the access frequency of chunks to decrease the response time. This method is connected with replica management that regulated the update policy for the new duplicated chunks achieving storage load balance. In recent times, most of the storage systems are designed to store replicated data for high availability. The storage systems do not provide any indicating that they are storing more than one copy of data. Cloud Storage servers look like they are storing more than one copy but the truth is they will be storing only a single copy. This problem can be overcome by using multiple-replica provable data possession (MR-PDP) [75]. It allows users to store copies of file to audit using a challenge-response protocol. MR-PDP is more efficient for storing replicas than a single replica PDP scheme. The fountain-code based cloud storage system i.e., Luby Transform (LT) has been proposed to explain the delay that happens during file retrieval by Chaun [77].

Ping Hu et al., [78] investigate the minimization of storage cost when the user stores its data in multiple untruthful and unreliable clouds and derives a jointly optimal coding and storage allocation scheme, which achieves perfect secrecy with minimum cost. Banyal et al., [79] propose a system framework whose main component is proxy server to increase the data availability service. It manages the performances of cloud service provider and this proxy server is used as middleware in between CSP and user. In order to provide space for large amount of data in less area, Pallavi et.al., [80] propose a framework that uses the AES data compression techniques to store huge amount of data in less space.

Zhenyu et al., [81] uses the Bell-LaPadula Multi-Level security model to achieve communication between clouds, reduce the computing power cost and also gives security to the data storage. The different data available techniques under cloud storage are shown in Table 4.

3. DATA PRIVACY

Securing user's personal information for any purpose without permission is called User Privacy [82]. Cui et al., [83] addresses the issues in privacy-preserving data sharing which allocates the single key to the client while sharing huge number of documents. Later, the user submits a single trapdoor when all the documents inquired by the owner.

Po-Wen et al., [84] achieves user privacy in implementing the fake user secrets and convince them to use secrets by proposing a new cloud storage encryption scheme. Wang [85] proposed XOR secret sharing schemes to propose privacy preserving data distribution schemes which permits computation over encrypted texts but difficult to prevent collusion attacks.

Kalyani et al., [86] improve the present Attribute-Based Encryption (ABE) [87] [88] to manage deletion or revoking of the user on demand efficiently. Data is secured and also access control policy is also achieved. It uses IDEA, Key Policy Attribute based Encryption(KP-ABE) [89] [90] [91] that focuses on access control policy and also uses Proxy Re-Encryption (PRE) [92], [93] to deliver the work of decryption key distribution to the cloud server.

Jin et al., [94] propose Key-Policy Attribute-Based Broadcast Encryption scheme (KP-ABBE) which uses double encryption process using both attribute-based encryption and broadcast encryption system. Constant-size public parameters is achieved by imposing no limit on the size of attribute sets used for encryption and has a large attribute universe. Nabeel [95] also uses double encryption to reduce the overhead on users. Lazy Revocation is also used for user revocation.

Table 5. Comparison of Different Data Privacy Techniques

Author	Algorithm	Performance	Advantages	Disadvantages
Yongge et al., 2015 [90]	MDS Code, BP-XOR codes, LDPC secret sharing scheme	Achieves privacy and reliability without employing encryption techniques		Hard to prevent collusion attacks
Shulan et al., 2016 [93]	Attribute based data sharing scheme	Confidentiality in data and privacy is achieved	High efficiency and security	
Jigco et al., 2016 [100]	Keyword Search Function, Outsourced ABE(OABE)	Cloud Service Provider performs partial decryption task delegated by data user without knowing anything about plaintext and keywords embedded in trapdoor	Secure against chosen-plaintext attack	Does not provide verifiability

By combining all these cryptographic techniques a secure data exchange through cloud is achieved and also minimizes the overhead on data owner. Fine-grained Attributes-based Access Control (ASPs) policy is used to select the share documents in public cloud. ACPs are used to manage the keys, outsourced the encrypted data.

Sherman et al., [96] uses homomorphic encryption scheme. Elliptic Curve Cryptography (ECC) is used to encrypt the data and shared with the TPA. ECC provides efficient that leads to fast computation time, power reduction. ECC is used to save the storage and bandwidth. Arockia [97] use the technology of virtualization that supports virtual machine consolidation and migration which intern improve the server utilization, availability, fault tolerance and energy efficiency. The data Privacy techniques under cloud storage are shown in Table 5.

4. MOBILE CLOUD DATA STORAGE SECURITY AND PRIVACY

Mobile Cloud Storage (MCS) [98] is the primary file storage mobile devices. The key element of the cloud is to maintain the growing amount of work and using the resource efficiently. Vaquero et al., [99] define cloud as a large pool where the user can access the virtualized resources. These resources are randomly reconfigured to permits the optimum resource utilization. Neeraj et al., [100] propose a Bayesian Coalition Game (BCG) as a service for RFID-based secure QoS management in mobile cloud. Khan et al., [101] describe Smart phones that support many applications which demands for increasing computational power. To overcome smart-phone constraints, researchers extends there cloud computing services to mobile devices also. The main challenge is to support the development of applications that can absorbes the features of cloud and requires specialized mobile cloud application models.

Sun [102] tell about the major challenges that are yet to be facing while using cloud based services in mobile devices are code/computation offloading, task-oriented cloud services, elasticity and scalability, security and cloud pricing. Trust management is used to support mobile cloud computing [103] [104] especially for an ad hoc mobile cloud. It has mobile nodes as resource providers without involvement of remote cloud.

Awad et al., [105] solves the problem of providing security to the outsourcing data by using the chaotic fuzzy transformation method from user devices to the cloud. The scheme also supports the fuzzy keyword searching. It maintains privacy and confidentiality of the user data by creating a secure posting list to rank the matched results and also saves resources of the user mobile devices. Priya et al., [106] enhances the existing search by using multi keyword search to reduce the communication cost. For securing the inner product computation multi keyword ranked keyword search (MRSE) [107] has been used. The challenging problem in applying efficient multi keyword fuzzy search on encrypted data is discussed in [108]. This scheme removes the predefined keyword dictionary. Each keyword is connected to its bigram vector representation and to capture keyword similarity, Euclidean distance is used.

Yu and Wen [109] propose a model where few functionality of mobile is moved of-device, so that it significantly reduces the usage of CPU, mobile resources. Once the functionality is moved to cloud, more resources are available in mobile. Few challenges [110] are resource constrain, attack on mobile, considering particular architecture depending on the platform used, Insignificance network and platform, mobile usability. Due to resources scarcity in the smartphone and less knowledge of security from users, encryption is used and the authentication between two parties depends on TPA. Zegers et al., [111] propose a lightweight encryption algorithm and a security handshaking protocol for mobile devices and data security is achieved from client side before it is sent to cloud. This method does not require a third-party authority for mutual communication and achieves minimum communication overhead.

When we need to store the data on the cloud, the process always begins from indexing it and symmetric encryption key using attribute based encryption. In searchable encryption scheme [112], the encryption for index is done by using

1) For every keyword, token is given for the encrypted files that contain keyword pointers that is retrieved and

2) The index is hidden when the tokens are hidden. The one who have the knowledge of secret key can only generate the tokens.

Searchable encryption uses Boolean keyword searches [113] for improving the efficiency while searching tree based index structure and multi-dimensional algorithm have been adopted that is better when compared to linear search. While retrieving the data from the cloud, relevance ranking is used. Such ranking helps in retrieving the information very quickly and it also removes the traffic in the network by sending only the relevant data to the user. To make searching more flexible for the user, Multiple keyword search [114] [115] is used. Multiple keyword search uses more than one keyword for searching. While using Multi keyword search, Sun et al., [116] makes use of Co-ordinate matching method. It matches to improve the relevance. The concept of inner query similarity has been used which provides the number of keyword that has been queried appearing in the document. Sometimes privacy is violated by the cloud vendor; vendors authorized users, unauthorized users or some external malicious entities. Using encryption methods becomes more complicated and expensive for mobile devices to manage privacy of stored cloud data.

Mehdi and Mukesh [117] propose a new light-weight method and makes use of pseudo-random permutation based chaos systems to store data in multiple clouds for mobile clients. The proposed system divides each files into multiple fragments and distributes each fragment to multiple files based on chaos system. It achieves low computation overheads and avoids unauthorized users including cloud entities.

Tysowski and Hasan [118] propose an efficient and highly scalable security in a cloud computing, where keys are managed by the client for achieve trust and key redistribution is minimized to reduce communication costs on mobile devices.

5. CONCLUSION

Cloud computing gives many advantages like storage security, increase storage space and reduce storage cost and decreases overheads on cloud, users. Proving the security to the data placed in cloud computing has become major issue in this IT platform. This paper mainly concentrates on security and privacy issues and also discusses about the different techniques used in existing cloud environments. Further, these different techniques are used in improving the security of the data stored and also giving privacy to the data.

6. REFERENCES

[1] P. Mell and T.Grance, "The NIST Definition of Cloud Computing", Natinal Institute of Standards and Techology, vol. 53, no.6, pp. 1-3, 2009.

[2] Leonard Heilig and Stefan Vob, "A Scientometric Analysis of Cloud Computing Literature", IEEE Transactions on Cloud Comouting, vol. 2, no. 3, pp. 266-278, July-September 2014.

[3] Cohen, Reuven, Rebello and Jagdish, "The State of Cloud Storage: A Benchmark Comparison of Speed, Availability and Scalability", White paper, Nausni, 2015.

[4] J. J.Wylie, M. Bakkaloglu, V. Pandurangan, M.W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, "Selecting the Right Data Distribution Scheme for a Survivable Storage System", Carnegie Mellon University, Technical Report, May 2001.

[5] Linlin Wu, Saurabh Kumar Garg, Steve Versteeg, and Rajkumar Buyya, "SLA-Based Resource Provisioning for Hosted Software-as-a-Service Applications in Cloud Computing Environments", IEEE Transactions on Services Computing, vol. 7, no. 3, pp. 465-485, July-September 2014.

[6] K. Hashizume, D. G. Rosado, E. Fernndez-Medina and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1-13, 2013.

[7] G. Kappes, A. Hatzieleftheriou and S. V. Anastasiadis, "Dike: Virtualization-Aware Access Control for Multitenant Filesystems", University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[8] Srinivasa Rao Chintada, ChandraSekhar Chinta, "Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments", International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 3, pp. 3609-3616, March 2014.

[9] Kevin D Bowers, Ari. Juels and Alina Oprea, "HAIL: A High Availability and Integrity Layer for Cloud Storage", In the Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, pp. 187-198, 2009.

[10] Spillner J, Mller J and Schill A, "Creating Optimal Cloud Storage Systems", IEEE Transactions on Utility and Cloud Computing, vol. 29, issue. 4, pp. 1062-1072, June 2013.

[11] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach and Security Challenge", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 1, pp. 421-424, March 2012.

[12] Victor Chang, Muthu Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transaction on Service Computing, vol. 9, issue. 1, pp. 138-151, ISSN: 1939-1374, January 2016.

[13] Kalpana Batra, Ch. Sunitha, Sushil Kumar, "An Effective Data Storage Security Scheme for Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no. 4, pp. 808-815, June 2013.

[14] Hamdan M. Al-Sabri, Saleh M. Al-Saleem, "Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security", IJCSI International Journal of Computer Science Issues, vol. 10, no. 1, pp. 259-266, March 2013.

[15] Keiko Hashizume, David G Rosado, Eduardo Fernndez-Medina and Eduardo B Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, pp. 1-13, 2013.

[16] Dan Boneh, Xuhua Ding and Gene Tsudik, "Fine-grained Control of Security Capabilities", ACM Transactions on Internet Technology (TOIT), vol. 1, no. 4, pp. 60-82. 2004.

[17] Raghavendra S, Girish S, Geeta C M, Rajkumar Buyya, Venugopal K R, S S Iyengar and L M Patnaik, "IGSK: Index Generation on Split Keyword for Search over cloud data", In the Proceedings of International Conference on Computing and Network Communications (CoCoNet), pp. 374-380, 2015.

[18] Danwei Chen and Yanjun He, "A Study on Secure Data Storage Strategy in Cloud Computing", Journal of Convergence Information Technology, vol. 5, no. 7, pp. 175-179, September 2010.

[19] Parakh A and Kak S, "Online Data Storage using Implicit Security", International Journal of Information Sciences, vol. 179, no. 19, pp. 3323-3331, 2009.

[20] Mohamed Ali, Kashif Bilal, Sharifullah Khan, Bharadwaj Veeravalli, Kaicheng Li and Albert Zomaya, "DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security", IEEE Transactions on Cloud Computing, ISSN: 2168-7161, 2015.

[21] K Badya Nayak, D Krishna, P Ravindra, "Data Integrity and Dynamic Storage Way in Cloud Computing", International Journal of Innovative Technologies vol. 3, issue. 2, pp. 0268-0273, ISSN: 2321-8665, June 2015.

[22] Ananda S. Hiremath, Shivaputra S. Panchal, Shriharsha S. Veni, "Providing Security for Data Storage in Cloud through Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, pp. 379-384, July 2014.

[23] Abhishek Patel, Prabhat Dansena, "TPM as a Middleware for Enterprise Data Security", International Journal of Computer Science and Mobile Computing, vol. 2, no. 7, pp. 327-332, July 2013.

[24] Matthew Malensek, Sangmi Pallickara, and Shrideep Pallickara, "MINERVA : Proactive Disk Scheduling for Qos in Multi-tier, Multi-tenant Cloud Environments", IEEE Transactions on Internet Computing, vol. 20, no. 3, pp. 19-27, ISSN: 1089-7801, May-June 2016.

[25] Xu, Lei and Wu, Xiaoxin and Zhang, Xinwen, "CL-PRE: A Certificateless Proxy Re-encryption Scheme for Secure Data Sharing with Public Cloud", In the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 87-88, 2012.

[26] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage", IEEE Transaction on Informations Forensics and Security, vol. 10, no. 9, pp.1981-1992, September 2015.

[27] R. Bala Chandar, M.S Kavitha, K seenivasan, "A Proficient Model for High end Security in Cloud Computing", ICTACT Journal on Soft Computing, vol. 4, pp. 694-702. January 2014.

[28] Neha Tirthani, Ganesan R, "Data Security in Cloud Architecutre based on Diffie Hellmam and Elliptic Curve Cryptography, IACR Cryptology e-Print Archive, 2013.

[29] Chen Yang, Furong Wang and Xinmei Wang, "Efficient Mediated Certificates Public-Key Encryption Scheme without Pairings", In the Proceedings of International Conference on Advanced Information Networking and Applications Workshops, AINAW, vol. 1, pp. 109-112, 2007.

[30] Mokhtarnameh, Razieh and Ho, Sin Ban and Muthuvelu, Nithiapidary, "An Enhanced Certificateless Authenticated Key Agreement Protocol", In the Proceedings of 13th International Conference on Advanced Communication Technology (ICACT), pp. 802-806, 2011.

[31] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", Transactions on Cloud Computing, ISSN: 2168-7161, August 2015.

[32] Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang, and Hai Jin, "Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email", IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, January 2016.

[33] Hou, Mengbo and Xu, Qiuliang, "Two-Party Authenticated Key Agreement Protocol from Certificateless Public Key Encryption Scheme", In the Proceedings of International Conference on Management of e- Commerce and e-Government, ICMECG, pp. 440-444, 2009.

[34] Chase, Melissa, "Multiauthority Attribute based Encryption", In the Proceedings of 4th Conference on Theory of Cryptography, pp. 515- 534, 2007.

[35] Sun, Yinxia and Zhang, Futai, "Secure Certificateless Public Key Encryption without Redundancy", IACR Cryptology ePrint Archive, p. 487, 2008.

[36] Deepanchakaravarthi, Purushothaman and Sunitha Abburu, "An Approach for Data Storage Security in Cloud Computing",International Journal of Computer Science Issues, vol. 9, no 1, pp. 100-105, March 2012.

[37] Zebin Wu, Yonglong Li, Antonio Plaza, Jun Li, Fu Xiao, and Zhihui Wei, "Parallel and Distributed Dimensionality Reduction of Hyperspectral Data on Cloud Computing Architectures", IEEE Journal of SelectedTopics in Applied Earth Observations and Remote Sensing, 2016.

[38] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, and Ruitao Xie, "DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems", IEEE Transactions on Information and Forensics and Security, vol. 8, no. 11, pp. 1790-1801, November 2013.

[39] Lars Bremer and Kalam Graffi, "Symbiotic Coupling of P2P and Cloud Systems: The Wikipedia Case", In the Proceedings of IEEE International Conference on Communication, pp. 3444-3449, 2013.

[40] Heng He, Ruixuan Li and Xinhua Dong and Zhao Zhang, "Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud", IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.

[41] Garcia-Rodriguez, Gerardo, and Francisco de Asis Lopez-Fuentes, "A Storage Service based on P2P Cloud System", Advances in Information and Technology, pp. 89-96, 2014.

[42] Kavalionak, Hanna and Montresor, Alberto, "P2P and Cloud: A Marriage of Convenience for Replica

Management", Self-Organizing Systems, pp. 60-71, 2012.

[43] Babaoglu, Ozalp Marzolla, Moreno Tamburini, Michele, "Design and Implementation of a P2P Cloud System", In the Proceedings of 27th Annual ACM Symposium on Applied Computing, pp. 412-417, 2012.

[44] Jin Li, "Erasure Resilient Codes in Peer-to-Peer Storage Cloud", In the Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 4, pp. 4-6, 2006.

[45] Sanghamitra De, Mridul Sankar Barik, Indrajit Banerjee, "Goal based Threat Modelling for Peer-to-Peer Cloud" 2016.

[46] Rajiv Ranjan, Liang Zhao, Xiaomin Wu, Anna Liu, Andres Quiroz and Manish Parashar, "Peer-to-peer Cloud Provisioning: Service Discovery and Load-Balancing", Cloud Computing, pp. 195-217, 2010.

[47] Azad F Barsoum and Aftab Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems",IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385, 2013.

[48] Kaiping Xue and Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing", IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459-470, 2014.

[49] N Jenefa and N Jayalaxmi, "A Cloud Storage System with Data Confidentiality and Data Forwarding", International Journal of Soft Computing and Engineering, vol. 3, March-2013.

[50] Hsiao-Ying Lin and Wen-Guey Tzeng, "A Secure Erasure Code based Cloud Storage System with Secure Data Forwarding", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, 2012.

[51] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", In the Proceedings of Network Distributed System Security Symposium, 2005.

[52] Mazhar Ali, Saif Malik, and Samee Khan, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing, 2015.

[53] Jayant D Bokefade, Audhut S, Bhise Prajakta A, Satarkar Dattatray G.Modani, " Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption", In the Proceedings of 12th International Multi-Conference on Information Processin, vol. 89, pp. 43-50 2016.

[54] Lihong Jiang, Li Da Xu, Hongming Cai, Zuhai Jiang, Fenglin Bu and Boyi Xu, "An IoT-oriented Data Storage Framework in Cloud Computing Platform",IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1443-1451, 2014.

[55] Yang Tang, Patrick PC Lee, John CS Lui and Radia Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion", Security and Privacy in Communication Networks, pp. 380-397, 2010.

[56] Aditya Kaushal Rajan, Vijay Kumar and Muzzammil Hussain, "Security Analysis of Cloud Storage with Access Control and File Assured Deletion (FADE)", Second International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 453-458, 2015.

[57] Ashfia Binte Habib, Tasnim Khanam and Rajesh Patil, "Simplified File Assured Deletion (SFADE)-A User Friendly Overlay Approach for Data Security in Cloud Storage System", International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1640-1644, 2013.

[58] Hui Tian, Yuxiang Chen, Chin-Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen, Jin Liu, "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE Transactions on Service Computing, 2015.

[59] Zhenyu Wen, Jacek Caa, Paul Watson, and Alexander Romanovsky, "Cost Effective, Reliable and Secure Workflow Deployment over Federated Clouds", Transactions on Services Computing, vol. 13, no.9, pp. 604-612, September 2014.

[60] A. Mei, L. V. Mancini, and S. Jajodia, Secure Dynamic Fragment and Replica Allocation in Large-Scale Distributed File Systems, IEEE Transactions on Parallel and Distributed Systems, vol. 14, no. 9, pp. 885-896, 2003.

[61] Zhongyuan Zhao, Mugen Peng, Zhiguo Ding, Wenbo Wang, and H. Vincent Poor, "Cluster Content Caching: An Energy-Efficient Approach to Improve Quality of Service in Cloud Radio Access Networks", IEEE Journal on Selected Areas in Communications, 2016.

[62] Qian Wang, Cong Wang, Jin Li, Kui Ren and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", Computer Security–ESORICS, pp. 355-370, 2009.

[63] Amol S. Choure S. M. Bansode, "A Comprehensive Survey on Storage Techniques in Cloud Computing", International Journal of Computer Applications, vol. 122, no. 18, pp. 3-25, July 2015.

[64] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel And Distributed Systems, vol. 25, no. 2, pp. 468-477, Febraury 2014.

[65] Dong Yuan, Yun Yang, Xiao Liu and JinJun Chen, "A Cost-Effective Strategy for Intermediate Data Storage in Scientific Cloud Workflow Systems", IEEE International Symposium on Parallel and Distributed Processing (IPDPS), pp. 1-7, 2010.

[66] Shubhashis Sengupta, Annervaz K M, Amitabh Saxena, Sanjoy Paul, "Data Vaporizer-Towards a Configurable Enterprise Data Storage Framework in Public Cloud", IEEE 8th International Conference on Cloud Computing, pp. 73-80, 2015.

[67] Rajat Saxena, Somnath Dey, "Cloud Audit: A Novel Approach for Data Intergrity Verification in Cloud Computing", In the Proceedings of International Conference on Secuirty in Computer Networks and Distributed Systems, pp. 1-15, 2016.

[68] Leena H.U, Premasudha B.G, Basavaraja P.K, "Sensible Approach for Soil Fertility Management using GIS Cloud", 2016.

[69] Huaqun Wang, Debiao He, and Shaohua Tang, "Identity Based Proxy- Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud", IEEE Transaction on Information Forensics and Security, vol. 11, no. 6, pp. 1165-1176, June 2016.

[70] Li Mingqiang, Qin Chuan, Li Jingwei and Lee Patrick, "CDStore: Toward Reliable, Secure and Cost-Efficient Cloud Storage via Convergent Dispersal", In the Proceedings of USENIX Annual Technical Conference (USENIX ATC, pp. 111-124, July 2015.

[71] Seungyeop Han, Haichen Shen, Taesoo Kim, Arvind Krishnamurthy, Thomas Anderson, and David Wetherall, "MetaSync: Coordinating Storage Across Multiple File Synchronization Services", IEEE Internet Computing, 2016.

[72] Yang, Zhi and Zhao, Ben Y and Xing, Yuanjian and Ding, Song and Xiao, Feng and Dai, Yafei, "AmazingStore: Available, Low-cost Online Storage Service Using Cloudlets", vol. 10, no. 6 pp. 1-5, 2010.

[73] Zhongyuan Zhao, Mugen Peng, Zhiguo Ding, Wenbo Wang, and H. Vincent Poor, "Cluster Content Caching: An Energy-Efficient Approach to Improve Quality of Service in Cloud Radio Access Networks", IEEE Journal on Selected Areas in Communications, vol. 34, no. 5, pp. 1207-1221, ISSN: 0733-8716, 2016.

[74] Xu, Xiaolong and Tu, Qun, "Data Deduplication Mechanism for Cloud Storage Systems", In the Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 286-294, 2015.

[75] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple- Replica Provable Data Possession", International Conference on Distributed Computing Systems, pp. 411-420, 2008.

[76] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei Dai, "CHARM: A Cost-Efficient Multi-Cloud Data Hosting Scheme with High Availability", IEEE Transactions on Cloud Computing, vol. 3, no. 3, pp. 372-386, July-September 2015.

[77] Haifeng Lu, Chuan Heng Foh, Yonggang Wen and Jianfei Cai, "Delay- Optimized File Retrieval under LT-Based Cloud Storage" IEEE Transactions on Cloud Computing, ISSN: 2168-7161, 2015.

[78] Ping Hu, Chi Wan Sung, Siu-Wai Ho, and Terence H. Chan, "Optimal Coding and Allocation for Perfect Secrecy in Multiple Clouds", IEEE Transaction on Information Forensics and Secuirty, vol. 11, no. 2, pp. 388-399, February 2016.

[79] R K Banyal, V K Jain and Pragya Jain, "Data Management System to Improve Security and Availability in Cloud Storage", 2015 International Conference on Computational Intelligence and Networks (CINE), pp. 124-129, 2015.

[80] Pallavi Srivastava and Navish Garg, "Secure and Optimized Data Storage for IoT through Cloud Framework", International Conference on Computing, Communication and Automation (ICCCA), pp. 720-723, 2015.

[81] Zhenyu Wen, Jacek Caa, Paul Watson, and Alexander Romanovsky, "Cost Effective, Reliable and Secure Workflow Deployment over Federated Clouds", IEEE Transactions on Services Computing, 2016.

[82] Abdul Sattar Raja and Dr. Shukor Abd Razak, "Analysis of Security and Privacy in Public Cloud Environment", International Conference on Cloud Computing, pp. 1-6, April 2015.

[83] Baojiang Cui, Zheli Liu and Lingyu Wang,"Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on Computers, vol. 6, no. 1, Jnauary 2014.

[84] Chi, Po-Wen and Lei, Chin-Laung, "Audit-Free Cloud Storage via Deniable Attribute-based Encryption", IEEE Transactions on Cloud Computing, ISSN: 2168-7161, April 2015.

[85] Yongge Wang, "Privacy-Preserving Data Storage in Cloud Using Array BP-XOR Codes", IEEE Transactions on Cloud Computing, vol. 3, no. 4, pp. 425-435, October-December 2015.

[86] Kalyani, Hulawale and Rahul, Paikrao and Ambika, Pawar, "Achieve Fine Grained Data Access Control in Cloud Computing using KP-ABE along with Lazy and Proxy Re-encryption", International Journal of Emerging Technology and Advanced Engineering, vol. 4, issue. 2, pp. 457-461, Febraury 2014.

[87] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data", In the Proceedings of 13th ACM Conference on Computer and Communications Security, pp. 89-98, 2006.

[88] Shulan Wang, Kaitai Liang, Joseph K. Liu, Member, IEEE, Jianyong Chen, Jianping Yu, Weixin Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016.

[89] Jin Sun, Yupu Hu, and Leyou Zhang, "A Key-Policy Attribute-Based Broadcast Encryption", The International Arab Journal of Information Technology, vol. 10, no. 5, pp. 444-453, September 2013.

[90] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable and Finegrained Data Access Control in Cloud Computing", In the Proceedings of INFOCOM, pp. 1-9, ISSN: 0743-166X, 2010.

[91] Sun, Jin and Hu, Yupu and Zhang, Leyou, "A Key-Policy Attribute based Broadcast Encryption", The International Arab Journal of Information Technology, vol. 10, no. 5, pp. 444-452, 2013.

[92] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography", Proceedings of EUROCRYPT, pp. 127-144, 1998.

[93] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable Secure File Sharing on Untrusted Storage", In the Proceedings of FAST, vol. 3, pp. 29-42, 2003.

[94] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han, "Flexible and Fine-Grained Attribute-

Based Data Storage in Cloud Computing", IEEE Transactions on Services Computing, ISSN: 1939- 1374, January 2016.

[95] Nabeel, Mohamed and Shang, Ning and Bertino, Elisa, "Privacy Preserving Policy-based Content Sharing in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2602–2614, 2013.

[96] Cong Wang, Sherman S.M.Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage", IEEE transaction on Computers, vol. 62, no. 2, pp. 362-375, February 2013.

[97] Arockia Ranjini A, Arun S, " A Comparison Study of Various Virtual Machine Consolidation Algorithms in Cloud Datacenter", vol. 78, pp.491-498, 2016.

[98] Li, Jie and Ma, Ronghua and Guan, Haiyan, "Tees: An Efficient Search Scheme over Encrypted Data on Mobile Cloud", IEEE Transactions Cloud Computing, 2015.

[99] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.

[100] Neeraj Kumar, Rahat Iqbal, Sudip Misra, Joel J. P. C. Rodrigues, M.S. Obaidat, "Bayesian Cooperative Coalition Game as-a-Service for RFID-Based Secure QoS Management in Mobile Cloud", IEEE Transactions on Emerging Topics in Computing, ISSN: 2168-6750, March 2016.

[101] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A Survey", Future Generation Computer Systems, vol. 29, no. 5, 2013, pp. 1278-1299, 2012

[102] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analysing Security, Privacy and Trust Issues in Cloud Computing Environments", Procedia Engineering, vol. 15, pp. 2852-2856, 2011.

[103] Vishwa Kiran S, Ramesh Prasad, Thriveni J, Venugopal K R, L M Patnaik, "Mobile Cloud Computing for Medical Applications", pp. 1-6, ISBN: 978-1-4799-5364-6, 2015.

[104] Vishwa Kiran S, Raghuram S, Thriveni J, Venugopal K R, "Efficient Video Transfer using LAN Caching assisted by Cloud Computing", TENCON 2015-2015 IEEE Region 10 Conference, pp. 1-5, ISSN: 2159-3450, January 2016.

[105] Abir Awad , Adrian Matthews, Yuansong Qiao and Brain Lee,"Chaotic Searchable Encryption for Mobile Cloud Storage", IEEE Transactions on Cloud Computing, ISSN: 2168-7161, 2015.

[106] Veerabathina Santi Priya, B Venkata Ramana and Smita Rani Shahu, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", International Journal of Scientific Engineering and Technology Research, vol. 04, issue. 11, pp. 2030-2032, May 2015.

[107] S Raghavendra, Nithyashree K, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik, " FRORSS: Fast Result Object Retrieval using Similarity on Cloud", in the proceedings of International Conference on Distributed Computing, VLSI, Electrical Circuts and Robotics (DISCOVER), 2016.

[108] Bing Wang, Shucheng Yu, Wenjing Lou and Y Thomas Hou, "Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud", INFOCOM, 2014 Proceedings IEEE, pp. 2112-2120, 2014.

[109] X. Yu and Q. Wen, "Design of Security Solution to Mobile Cloud Storage", in Knowledge Discovery and Data Mining. Springer pp. 255-263, 2012.

[110] D. Huang, "Mobile cloud computing", IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, vol. 6, no.10, pp.27-31, 2011.

[111] William Zegers, Sang-yoon Chang, Younghee park and Jerry Gao, "A Light-Weight Encryption and Secure Protocol for Smartphone Cloud", IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 259-266, 2015.

[112] S. Kamara and K. Lauter, "Cryptographic Cloud Storage", Financial Cryptography and Data Security. Springer, pp. 136-149, 2010.

[113] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward Privacy-Assured and Searchable Cloud Data Storage Services", IEEE Transactions on Network, vol. 27, no. 4, pp. 56-62, 2013.

[114] S Raghavendra, C M Geeta, Rajkumar Buyya, Venugopal K R, S S Iyengar and L M Patnaik, "DRSMS: Domain and Range Specific Multi-Keyword Search over Encrypted CLoud Data", in the International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no. 5, ISSN: 1947-5500, May 2016.

[115] S Raghavendra, Doddabasappa P A, C M Geeta, Rajkumar Buyya, Venugopal K R, S S Iyengar and L M Patnaik, "Secure Multi-Keyword Search and Multi-User Access Control over an Encrypted Cloud Data", International Journal of Information Processing (IJIP), vol. 10, no. 2, ISSN:0973-8215, 2016

[116] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-based Ranking", 8th ACM SIGSAC Symposium on Information, Computer and Communications Security Proceedings, pp. 71-82, 2013.

[117] Mehdi Bahrami and Mukesh Singhal, "A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing", 3rd IEEE International Conference on Mobile Cloud Computing, Services and Engineering (MobileCloud), pp. 189-198, 2015.

[118] Piotr K Tysowski and M Anwarul Hasan, "Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds", IACR Cryptology ePrint Archive, pp. 668-678, 2011.