International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

Secure Data Sharing in Cloud Computing: A Comprehensive Review

Muthi Reddy P.[a]*, Manjula S. H.[b] , Venugopal K. R.[c]

[a,b,c]*Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bangalore University, Bengaluru-560001, India*

[a]*Email: muthireddy2016@gmail.com*

[b]*Email: shmanjula@gmail.com*

[c]*Email: venugopalkr@gmail.com*

Abstract

Cloud Computing is an emerging technology, which relies on sharing computing resources. Sharing of data in the group is not secure as the cloud provider cannot be trusted. The fundamental difficulties in distributed computing of cloud suppliers is Data Security, Sharing, Resource scheduling and Energy consumption. Key-Aggregate cryptosystem used to secure private/public data in the cloud. This key is consistent size aggregate for adaptable decisions of ciphertext in cloud storage. Virtual Machines (VMs) provisioning is effectively empowered the cloud suppliers to effectively use their accessible resources and get higher benefits. The most effective method to share information resources among the individuals from the group in distributed storage is secure, flexible and efficient. Any data stored in different cloud data centers are corrupted, recovery using regenerative coding. Security is provided many techniques like Forward security, backward security, Key-Aggregate cryptosystem, Encryption and Re-encryption etc. The energy is reduced using Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Data Centers.

Keywords: Encryption; Key-Aggregate; Backward Secrecy; Forward secrecy; Regenerative coding.

1. Introduction

Nowadays, Cloud Technology is a standout amongst the most conspicuous novelties, because of its cost-effectiveness and adaptability. It is received by vast organizations to have different service platforms viz., GoogleApps by Google, EC2 by Amazon, iCloud by Apple and so forth. Indalecio and his colleagues [1] describe the distributed (cloud) computing as a model for empowering omnipresent, advantageous, on-request network access to mutual configurable processing resources like servers, storage devices, networks and services.

----

* Corresponding author.

This can be rapidly implemented then discharged through insignificant services exertion or services supplier connection [2,3]. The general population uses to store their records at a reasonable cost or for free. The distinctive types of cloud service are Dropbox, Just cloud, Baidu container and Google drive, etc., [4]. Such environment gives client's not to claim the framework for different processing service. Indeed, they can be used to access data from any computer in any part of the world [5,6]. This consolidates the components supporting high versatility and multi-occupancy, offering high flexibility when compared with the earlier existing computing approaches. We compare the different parameters such as cloud security, data sharing, threads, algorithms, defense strategies, requirements and impacts on society as shown in Table 1.

Mauro and his colleagues [7] and Magyar and his colleagues [8] presents the improvement of proper mechanisms to lower the effect of Virtual Machine (VM) movements on the Service Level Agreement (SLA) working toward the implementation of prototype by depicting a approach of predictive control for energy-aware combination of VMs in a distributed computing infrastructure. This approach tells about virtual machines which are legitimately moved among physical machines to decrease the measure of dynamic units and it permits one to exchange among power savings and infringement of the service level agreement. The Cloud computing as one of the valuable platform which gives information to store on the databases at low prices and available over the web. One of the extensive scale cloud application is Infrastructure as a Service (IaaS). There is an absence of instruments that permits developers to associate various resource scheduling algorithm in IaaS related to mutually computing servers and client assignments. Distributed computing as Internet-based computing, thereby, mutual resources, programming and data is given to computers as well as devices [9].

Park and his colleagues [10] introduced the concept of Cloud Service Providers (CSPs) that uses a pay-per-use billing scheme in their pay-as-you-go pricing model. For example, the consumer uses as many resources as needed and is billed by the provider for the amount of resources consumed by the end of an agreed-upon period. CSPs usually guarantee the QoS in terms of a Service Level Agreement (SLA). Cloud pleasantries offer awesome comfort for that clients to appreciate the on-request cloud applications without considering the neighborhood framework confinements. Distributed computing implies essentially saving money on IT execution costs. Cloud offers more public door for new development and even distribution of whole enterprises. Distributed computing is the vision of processing as a utility; information proprietors can remotely store their information in the cloud, top notch applications and service from a common pool of configurable processing assets. Distributed computing can be derived in view of the services offered and deployment models [11,12].

The different types of services are defined by three layers as given below.

i) *Infrastructure as a Service (IaaS):* This layer is the lowest layer, to provide fundamental infrastructure support service.
ii) *Platform as a Service (PaaS):* It is the middle layer, which offers platform based services, providing the environment for facilitating client's applications.
iii) *Software as a Service (SaaS):* This layer is the topmost layer, which includes total applications offered as services on request.

Zhou and his colleagues [13] describe the cloud computing as a trustworthy information technology architecture which is applied to both enterprise and individuals. It provides shared processing resources, data to computers and other devices. Over the past few years, cloud computing advanced and augmented its trend by computing paradigm. It is built around concepts such as on-demand computing resources, location independent resources pooling, versatile scaling, and end of in advance capital and operational costs. It is made on building a pay-as-you-go business model for computing and data technology services, as well as the internet of service. In terms of health, the Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities and many other governments for efficient and high-quality medical treatment. Zhang and his colleagues [14] proposed an upper bound protection spillage constraint-based approach. To recognize which transitional informational collections should be encoded and which don't. Protection saving expense can be spared while the security necessities of information holders can even now be fulfilled. This protection safeguarding expense of intermediate informational indexes can be essentially diminished. This coordinates anonymization with encryption to accomplish security protecting of numerous informational indexes. This fails security mindful productive booking of the middle of the road informational indexes in the cloud by taking protection safeguarding as a metric together with different measurements, for example, stockpiling and calculation. The following parameters are required to satisfy the privacy of data.

i) *Authentication:* Liu and his colleagues [15] showed that the authorized client can get to its own information field. Further, protected path was used as Two Factor Authentication (2FA). This 2FA is exceptionally regular between e-Saving money managements. Despite a username/secret word, the client should have the gadget to show a One Time Password (OTP).

ii) *Data Anonymity:* Raja and his colleagues [16], Zhang and his colleagues [17] and Yu and his colleagues [18] discuss the unrelated entity that cannot recognize the exchanged data. Data aggregation either at a centralized location or at any one of the individual sites is also impractical due to communications and storage costs of big data. Data anonymization means hiding identity and delicate information which provides the secrecy of an individual is successfully safeguarded though certain data be able to still present to information clients for different examination and mining tasks. Efficient integrity auditing scheme supports checking, fault detection probability, multiuser alteration and user revocation.

iii) *User Privacy:* The data should not be accessed, until and unless both the users have the interest to share their respective data.

Shuang and his colleagues [19] propose a simple but efficient method to safeguard the reliability of user's information in the cloud. Members of the group can be offline temporarily and can be online at any time. The group can be negotiated by the efficient cloud servers by the support of group key pairs. The information shared in a group is protected with the Group key pairs. Before uploading data to the cloud, one should encrypt the file with encryption technique. When a group member negotiates from the group or a new member joins the group key pairs are updated. The temporary offline members of the group are also considered in updating group pair protocol. When these members of the group become online again then they should go through the key synchronization to get the updated key pairs. In Security model, the system should fulfill the security requirements of backward privacy and forward privacy, the group left member cannot decrypt new cipher text and a newly entered fellow can approach and decrypt the earlier distributed data respectively in [20]. Cloud computing atmosphere satisfies needs by producing VMs and allotting the resources to them in view of the needs of the applications, i.e., essential to set up them on the cloud atmosphere. These applications possibly will have a diverse arrangement and dissimilar structural design like social networking, informal communication, and web hosting. Virtualization tool can be used as a spirit of distributed computing lifespan and this is inadequate to actually existing resources. Thus exploitation of each and every resource plays major significant responsibility in dealing the distributed computing life-cycle powerfully, in turn, to organize these massive applications effectively and productively in cloud environments.

Motivation: The problem of different scheduling algorithms, to allocate resources for users and data security in distributed cloud data centers to evaluate their different metrics are as follows;

(a) Data security
(b) Data anonymity
(c) Data sharing
(d) Load balancing
(e) Avoid intruders
(f) Efficiency and
(g) Data storage

In distributed system data security is a major issue. Anonymity is property processed by certain anonymized data. Data sharing is very important in researchers, scientific, and government activities etc. Load balancing is a significant piece of distributed computing life cycle. The researchers have been anticipated this is the active load balance strategy has a number of constraints with respect to performance time and memory requirement.

2. Background

The sharing of data securely in cloud computing is a very crucial method. The information is stored in cloud data centers. To access data from or store data into data centers through the internet, the intruders may attack our data. To avoid attackers hacking data and proper utilization of resources, we discuss many algorithms and techniques.

Organization: The residue of this paper is structured as follows. Section 3 present the Architecture of secure data storing and resource sharing in the cloud. System Model is defined in section 4. Various Technologies of cloud computing are presented in chapter 5 and section 6, contains conclusions of secure information sharing in cloud computing.

3. Architecture

The architecture of secure data storing and resource allocation in Cloud Computing is shown in Figure 1. Different user's first register in the cloud. Security provider checks the authentication of the user to upload a file of the owner by generating a private key. The encrypted file is stored in the cloud server. Worldwide end clients access the file with permission of the respective file owner. Any file requested from the authorized user is checked by the availability of the resource in the cloud storage. The resources availability is stored in a separate file, i.e., called reliability check. The virtual machine allocates the resources or resources are not allocated. If the file is present, the end user easily receives the file or else if the file is corrupt then the file is regenerate and delivered to the end user based on demand. Security is provided by encrypting the private key in constant size.

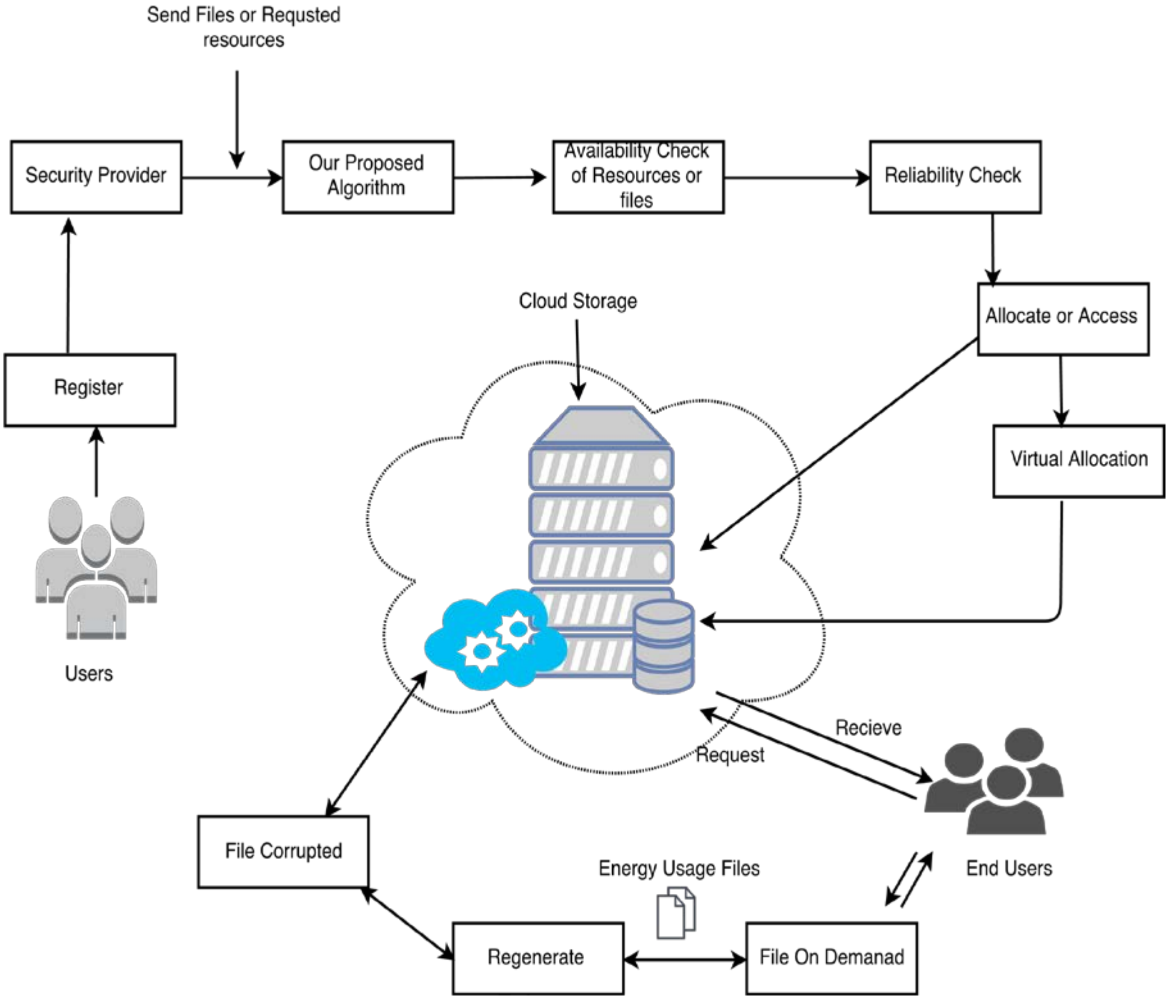

Figure 1: The Architecture of Secure Data Storing and Resource Allocation in Cloud.

4. System model

The file upload/download in a Cloud storage is shown in Figure 2. It illustrates the steps to secure, private and public data by generating the Key-Aggregate key. The data flow between users through data centers in a cloud server. The user can register and authenticate if the user exists. The authorized users can upload the file to the server. The server automatically generates a private key; the file is encrypted and stored on the servers. Any user can request to download a file initially by checking the availability of file and resources, and then the authorized user can download file by giving his private key. If the file is hacked by any intruder, another duplicate of the file stored in the distributed data center can be accessed. Here, we use a regenerative function to generate code of corrupted files. Most of the file access are based on client's demand.

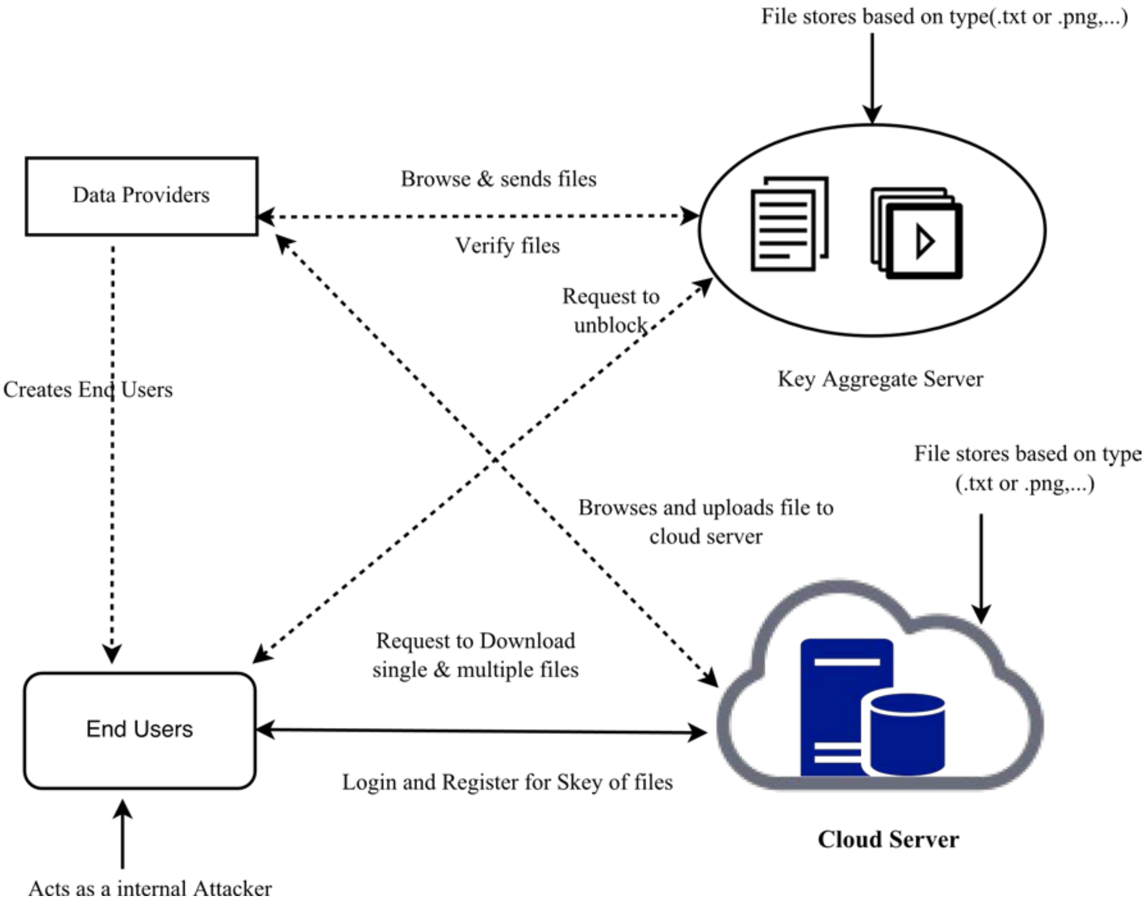
File stores based on type(.txt or .png,...)
Data Providers
Browse & sends files
Verify files
Request to unblock
Key Aggregate Server
Creates End Users
File stores based on type (.txt or .png,...)
Browses and uploads file to cloud server
Request to Download single & multiple files
End Users
Login and Register for Skey of files
Cloud Server
Acts as a internal Attacker

Figure 2: System Model: To Upload/Download a File in Cloud Storage.

5. Cloud Technology

In this section, we discuss various issues to provide data security, resource allocation and load balancing in a cloud computing environment.

5.1 Mobile cloud computing

Mobile cloud computing is an architectural pattern where information storage and CPU concentrated tasks are performed on cloud and cell phones are primarily utilized as a thin customer to associate with the application and rendering the outcomes handled from the cloud environment. The different techniques discussed as follows; Lazaros and his colleagues [21] advocated the requirement for novel cloud model and migration techniques that effectively brings the computation of the cloud nearer to the mobile user. It comprises of a back-end cloud and a local cloud, which is appended to remote access infrastructure. This can be outlined into various classes of task migration policies, spreading over completely clumsy ones. Every client or server independently settles on its relocation choices, up to the broad movement procedure of a cloud supplier [22].

Liang and his colleagues [23] proposed a solid plan fulfilling the new idea. A general idea for Proxy Re-Encryption (PRE), this is called as Deterministic Finite Automata Based functional PRE (DFA-based FPRE). The first and cement DFA-based FPRE framework, which adjusts to the new idea. In this plan, a message is encoded in a figure content related with a self-assertive length record string and a descriptor is genuine if and just if a DFA related with his/her mystery key acknowledges the string. This encryption is permitted to be changed to another figure content related to another string by a semi-trusted intermediary to whom a re-encryption key is given. Chu *and his colleagues* [24] demonstrates to proficiently, safely and adaptable impart information to others in distributed storage likewise the predefined bound of the quantity of most extreme ciphertext classes. The quantity of ciphertexts ordinarily develops quickly in the distributed storage. They portray new open key cryptosystems that create steady size ciphertexts to such an extent that ingenious task of decoding rights for any arrangement of ciphertexts is conceivable. This is extra versatile than different leveled key assignment which can simply keep spaces if each and every key-holder share a like course of action of advantages. Zhang *and his colleagues* [25] investigates the optimization of calculation cost on the Third-Party Auditor (TPA) side. It examine the folder of multiple cloud servers and multiple Cyber-Physical-Social System (CPSS) users. This is very costly for users to accumulate large data sets and causes trouble in data management. Therefore, it is serious importance to farm out the data to cloud servers, which provides users cost-effective, easy and flexible technique to deal with data. Proposed model is secure certificate less public integrity verification scheme Secure Certificate Less Public integrity Verification scheme (SCLPV). The first work that concurrently supports certificate less public verification and conflict against malicious auditors to prove the integrity of outsourced data in CPSS.

Liu *and his colleagues* [26] solves the challenging issue of sharing data in a multi-proprietor way through identity privacy and preserving data from an untrusted cloud, because of the repeated change of the enrollment. The author proposed a secure multi-owner information distribution pattern called Mona, in favor of active groups in the cloud. Here customer is competent to impart information to others in the group without enlightening uniqueness secrecy of the cloud. Furthermore, Mona provisions new customer joining and efficient customer revocation. The encryption computation cost, storage overhead are stable and it satisfies guarantees efficiency and desired security requirements as well. In [27], huge storage used for decoding passkey in resource-constraint devices such as smart voucher or cellular sensor, smartphones knob. Particularly, these undisclosed passkey are frequently stored in the tamperproof remembrance, whichever almost costly. The current analysis achievement essentially target on reduce the contact needs like frequency, looped of connection such as composite stamp. To overcome this difficulty by originate a unique form of open key encryption that entitle as Key Aggregate Cryptosystem (KAC). A comparable property displaying a stable size decoding key, however the classes have to be conventional to a few predefined hierarchical association. It is elastic in the sensibility that this control is eradicate, that is, not unique relationship is essential among the classes. The whole constructions can be established protected in the criterion model.

Liang *and his colleagues* [28] proposed various methods to protect the information stored in cloud can be achieved. These methods include Access Control policies and mechanisms, Proxy ReEncryption, Anonymous Access, Identity-Based Encryption, Attribute-Based Encryption, Searchable Symmetric Encryption and Auditing. Security in public cloud storage is of prime concern as the information is outsourced towards third party cloud package providers. This information may disclose unexpectedly due to malicious attacks on the cloud or careless management of cloud operators [29]. Hur *and his colleagues* [30] concentration on the key era focus could decode any messages tended to particular clients by producing their secretive keys. It is not appropriate for information sharing situations where the information proprietor might want to make their private information just available to assigned clients. What's more, applying Ciphertext Policy Attribute Based Encryption (CP-ABE) in the information imparting framework acquaints another test with respect to the client renouncement since the get to arrangements are characterized just above the quality world. A novel CP-ABE plot for an information distribution framework by misusing the normal for the framework engineering. Chow *and his colleagues* [31] attempts to enhance the spillage allowed from every private key as the portion of its size. Security analysis is more complicated so by designing the main Leakage Resilient Identity-Based Encryption (LR-IBE) frameworks of settled suspicions in the standard model. They determine these plans by applying a hash confirmation system to variations of the current IBE plans. Subsequently, spillage flexibility in the specific static suppositions of the first frameworks in the standard model, while likewise protecting the effectiveness of the first plans is accomplished.

Yuen *and his colleagues* [32] demonstrates that, it is difficult to keep away from all feasible kinds of leakage, like side-channel attacks that make use of the physical nature of cryptographic operations. Identity-Based Encryption (IBE) that remains protected even when the opponent is prepared with auxiliary input, any computationally unavoidable function of the identity-based secret key and the master secret key. Proposed model of Continual Auxiliary Leakage (CAL) which can capture both continual leakage and memory leakage. This structure is completely protected in the standard model based on only static assumptions, and can be easily unlimited to give the first hierarchical IBE with auxiliary input. The CAL model is mostly pleasing while it gives a clean definition when there are multiple secret keys. Raghavendra *and his colleagues* [33] introduces a new technique called multi-keyword search for accomplishing information utilization effectively through Internet over remotely stored encoded cloud information. On a large dataset Ranked Searchable Symmetric Encryption (RSSE) system is inefficient to accomplish search for multi-keyword ranked. To overcome this drawback a Domain and Range Specific Multi-Keyword Search (DRSMS) algorithm used. New domain provisions more effective and precise search. This algorithm reduces the ranked searchable encryption time and index storage space for top k multi-keyword recovery on cloud delicate data. Ruj *and his colleagues* [34] exhibited a decentralized access control system with unknown validation. It gives customer denial and anticipates replay attacks. In cloud doesn't know the identity of the customer who stores information, however just checks the customer's accreditations. Enter transport is done decentralized. One control is cloud knows the get the opportunity to approach for each record set away in the cloud. Its issues is to conceal the traits and access strategy of a client.

Wang *and his colleagues* [35] exploited before permit users to organize contact to their information stored in a public cloud, cloud providers enforce appropriate access manage policies and mechanisms. Generally access control can be divided into three types, they are as follows; i) Attribute-Based Access Control (ABAC), ii) User Based Access Control (UBAC) and iii) Role-Based Access Control (RBAC). In the UBAC model, the catalogue of consumers who are allowable to contact information are contained in the access control list. In RBAC representation, users are mapped to roles and access authorizations. For example, the roles are assigned to users based on their tasks along with credentials in the association and consents are consigned to these roles as a substitute of entity consumers. A role can be left permissions from other roles forming a hierarchy of roles. In ABAC model, users have attributes and information has right of entry rule. Sun *and his colleagues* [36] pointed out identity based encryption is an open key encryption, wherever the open key of a consumer has various exclusive data related to uniqueness of the consumer. Attribute-Based Encryption (ABE) is a kind of open key encoding wherein either the private key of a consumer or the ciphertext or mutually related with attributes. In the case of secret key of a user associated with a right of entry strategy, the key can be capable of decrypt a ciphertext related by means of attributes fulfilling the strategy. Proxy Re-Encryption (PRE) permits a third party to modify a ciphertext that has been encoded for single party, therefore it may be decrypted by any more. There are many variations of PRE for instance Conditional PRE, Identity-Based PRE (IBPRE) and Attribute Based PRE (ABPRE). In Ciphertext Proxy Re-Encryption (CPRE), a ciphertext associated with a condition is converted to another ciphertext with another condition. IBPRE and ABPRE are quite similar, the difference being ABRE more expressive. Searchable Symmetric Encryption (SSE) enables search on ciphertext. In the first Searchable Encryption (SE) scheme proposed, a user has to go through the entire document to search for a particular keyword in the document. Two Round Searchable Encryption (TRSE) design accomplishes the protected multi-keyword top-k recovery encrypted cloud information [37].

Yang *and his colleagues* [38] introduced the concept of Multi-Party Searchable Encryption (MPSE) design allows a user to construct an encrypted catalogue for the entry permit and upload it on top of a cloud server. This catalogue contains a register of encrypted keywords along with permission data that selectively authorizes users to explore over this catalogue. Auditing is necessary in the direction of checking the data integrity in cloud. A third-party assessor is usually the preference for storage space auditing on cloud. In auditing procedure, the owners must keep information private in opposition to the auditor that support active updates of the data in cloud and should also hold bunch auditing for several owners and various clouds. Anonymous access is used to preserve the privacy of users access request related information. Beaumont *and his colleagues* [39] considers a problem of resource allocation that models both virtual machines allocation and independent tasks scheduling problems. The goal is to find an allocation of the servers degree is greater than the number of customers allocated to a server. Their request is littler than the limit of servers, while augmenting the overall throughput. The author proposed an algorithm SEQ that tells about resource augmentation to give a solution to Maximize Throughput Bounded Degree (MTBD) problem. The solution of the problem is a degree constraint, that is crucial for realism in both contexts several other greedy heuristics to solve the online problem. Bahga *and his colleagues* [40] proposed the fine-grained resource sharing can be able to achieve as each virtual machine substrate can be configured through appropriate shares of resources vigorously. In the cloud environment, the quantity of allotted resource scan be altered adaptively at a well granularity that is commonly mentioned towards auto-scaling. This auto-scaling skill of the cloud enriches source consumption through matching the supply with the demand. In cloud providers frequently used resources are CPU and memory.

Zaman *and his colleagues* [41] in order to generate higher profit, tended to the problem of dynamically provisioning Virtual Machine (VM) instances in clouds while finding the portion of VM with a combinatorial auction based system, called CA-PROVISION to tackle the issue and performed effective simulation experiments with actual workloads to assess. This mechanism assures the VMs dynamically and it does not require the evaluation of workload characteristics, rather the current demand for VMs is captured. In the fast development of Internet has fostered a large number of new technologies, including cloud computing. Cloud computing emerged as a Virtualization technology aims to provide scalable, transparent network resource to end users. The end users of cloud can access the on-demand computing and storage resource. Distribution of cloud environment; dynamic load scheduling module which proposes a hybrid load balance algorithm to realize high performance load balance for cloud center. Parikh *and his colleagues* [42] observes that the next generation server farm and permit specialist organization to make utilization of server farm limit gave by cloud and amplify the application in view of necessity of client. Server farm of this cloud computing has list of applications and large number of resources need to utilize those resource. This give dynamic load adjust approach in light of various parameter like memory required, execution time and mists registering surroundings to propel its execution by resource usage. Inside it utilizes Hungarian calculation for load adjusting with cost advancement and for demonstrating and reenactment CloudSim is utilized. Wu *and his colleagues* [43] proposed precedence advancement and dynamic time slice mechanisms. To decide the schedule Virtual CPUs (VCPUs) as indicated by the qualities of delicate real-time applications. Current hypervisors don't provide adequate provision because of synchronization problems and soft real-time constraints which result in frequent serious performance degradation and deadline misses. The main issue is CPU schedulers in underlying hypervisors. Design and implementations of a parallel soft real-time scheduler as indicated by the examination, named Poris, in view of Xen. It addresses both asynchronization problems and soft real-time constraints simultaneously.

Li *and his colleagues* [44] introduced the concept of dynamic load balancing algorithms recommend the prospect of getting better load distribution at the cost of supplementary communication and calculation expenses. Compared with the centralized strategies, distributed dynamic load balancing offers more advantages, such as scalability, flexibility and reliability. A novel multi-objective dynamic scheduling representation for urgent situation tasks on distributed imaging satellites is recognized for the first instance. To advance users fulfillment ratio and resource consumption, the task merging approach: establishing a Task Merging Graph (TMG) representation and proposing a task merging algorithm present a big confront to scheme and realize novel and quick dynamic scheduling algorithms for urgent situation tasks and developing an well-organized dynamic scheduling scheme found [45]. Cloud computing may be categorized based on the foundation of amenities accessible and consumption models. Du *and his colleagues* [46] proposed IntTest, an adaptable and viable administration uprightness validation system for SaaS clouds. IntTest suppliers a novel coordinated authentication chart examination plot that can give more grounded aggressor pinpointing power than preceding arrangements. IntTest can obviously upgrade result quality by supplanting dreadful outcomes delivered by vindictive aggressors with awesome outcomes created by generous specialist co-ops. IntTest can accomplish higher aggressor pinpointing exactness than present methodologies. IntTest does not require any extraordinary apparatus or secure piece reinforce and constraints slight execution impact to the application, which makes it viable for substantial scale cloud structure benefit respectability confirmation problem has not been properly addressed.

5.2 Integrity and Forward security

Integrity, regarding data and framework security, is the affirmation that information must be accessed or adjusted by those endorsed to do all things considered. Actions were taken to ensure integrity incorporate controlling the physical state of networked terminals and servers, restricting access to data and keeping up exhaustive authentication ones. Forward security is a property of secure correspondence conventions in which trade off of long term keys does not deal past session keys in cryptography. Forward secrecy ensures past sessions against future bargains of secret keys or passwords.

Table 1: Comparison of Related Works

Author	Cloud Security Yes/ No	Data Sharing Yes/ No	Algorithm	Threats Yes/ No	Defense Strategies Yes/ No	Requirements Yes/No	Impacts on Society Yes/No
Indalecio *and his colleagues* 2016, [1]	Yes	Yes	Apache CloudStacks interface	No	Yes	Yes	Yes
Mauro *and his colleagues* 2016, [7]	Yes	Yes	Optimal control and Predictive control, Energy-aware consolidati-on and Monte Carlo optimization	No	Yes	Yes	No
Dai *and his colleagues* 2016, [82]	Yes	Yes	MinES and MinCS yield scheduling	No	Yes	Yes	Yes
Li *and his colleagues* 2016, [83]	Yes	Yes	SecCloud	No	Yes	Yes	Yes
Heng *and his colleagues* 2016, [120]	Yes	Yes	Ciphertext-Policy Attribute-Based Encryption (ABE)	No	Yes	Yes	Yes
Nejad *and his colleagues* 2015, [8]	Yes	No	VCG-VMPAC Mechanism, G-VMPAC-X Mechanism, and G-VMPAC-X-ALLOC allocation	Yes	No	No	Yes
Elli *and his colleagues* 2015, [12]	Yes	Yes	Ambient Assisted Living (AAL) Technologies	No	Yes	Yes	Yes
Li *and his colleagues*	Yes	Yes	Bin packing, Cloud gaming, Play request	No	Yes	Yes	Yes

2015, [60]			dispatching and Service cost soft real-time				
Liu *and his colleagues* 2015, [79]	Yes	Yes	Cryptographic	Yes	Yes	Yes	Yes
Alasaad *and his colleagues* 2015 [92]	Yes	Yes	Optimum window sizes and optimum resource location in every window, Optimum resource allocation in the cloud using two resource provisioning plans	No	Yes	Yes	Yes
JIA *and his colleagues* 2015, [99]	Yes	Yes	Memory bandwidth and Soft real-time	No	No		Yes
Tian *and his colleagues* 2015, [132]	Yes	Yes	Scheduling Algorithms-Taking LIF Algorithm	No	Yes	No	Yes
Shuang *and his colleagues* 2014, [19]	Yes	Yes	KeyGen, SigGen, GenProof and CheckProof	Yes	Yes	No	No
Chu *and his colleagues* 2014, [24]	Yes	Yes	Setup(), KeyGen(), Encrypt(), Extract() and Decrypt()	No	Yes	Yes	Yes
Yuchuan *and his colleagues* 2014, [56]	Yes	Yes	Setup, SignBlock, Challenge, ProofGen and ProofVerify	No	Yes	Yes	Yes
Shuanbao *and his colleagues* 2014, [105]	Yes	Yes	Ciphertext-Policy Attribute-Based Encryption (CPABE)	No	Yes	No	Yes

Huang *and his colleagues* [47] addressed the problem of key demonstration is additional outrageous in a ring signature method: If a ring member's private key is revealed, the adversary can make considerable ring signature of some records for the benefit of that grouping. Surprisingly more dreadful, the grouping can be portrayed by the adversary willfully in view of the abruptness stuff of ring signature. This challenge simply essentials to fuse the exchanged off a customer in his preferred grouping. Accordingly, the performance of one customer's secret key renders all as of now got ring signatures invalid, since one can't perceive whether a ring signature is created before the key overview or by which customer. Subsequently, forward security is a vital necessity that a foremost information sharing structure must meet. Else, it wishes to provoke to a goliath pointless activity and resource. There exist countless calculations to give potential security and protection issues together with security architectures, information ownership protocols, and information public auditing protocols, secure information storage and information sharing protocols, get to control instruments, security safeguarding protocols, and key administration [48].

Bahga *and his colleagues* [49] proposed a model for protecting information privacy using visualization techniques based on screen space metrics. Under this sort of system, the transmission of individual information and authorization of the server in accessing the stored information represent the issue of security saving that is generally disregarded in the multimedia community. Hsu *and his colleagues* [50] solve the problem of the homomorphic comparison, Privacy Preserving Scale Invariant Feature Transform SIFT (PPSIFT), representation in the encoded domain and addresses secure SIFT feature extraction. As compared to the greater part of the processes in SIFT must be transmitted to the encoded domain. Proposed scheme is protection safeguarding acknowledgment of the SIFT format in light of homomorphic encryption. This results, security examination in view of the discrete algorithm issue and RSA that PPSIFT is secure against ciphertext just assault and known plaintext assault. Wang *and his colleagues* [51] presented the integrity of information in distributed storage is liable to examination, as the information put away in the cloud can undoubtedly be lost because of the unavoidable hardware/software failures and human mistakes. Despite the fact that outsourcing information to the cloud is cost effective for long haul substantial scale stockpiling, it doesn't offer any ensure on information uprightness and accessibility. In the event that these arrangements are reached out to bolster authors with information respectability confirmation, the information proprietor needs to remain the internet, gathering modified information from different clients and recovering validation labels for them [52,53].

5.3 Data confidentiality

Information security is basically that territory of the law that administers what may and what may not with individual data stored on the cloud. Wen *and his colleagues* [54] focus on managing data and the convergent key when users frequently update it and they planned to improve schemes to support data owner privacy preservation by a session-key-based concurrent key administration method, called SKC, to protected the dynamic overhaul in the information De-duplication. Proposed convergent key management schemes, SKC and Convergent Key Sharing (CKS) for cross-user data De-duplication in Cyber-Physical Social System (CPSS). In SKC, every information proprietor can confirm the rightness of the convergent key and in CKS can dynamically refresh the convergent key and support the several Local Communication Networks (inter-LCNs) data De-duplication without the help of Gateway (GW). Both techniques can protect the data confidentiality, convergent key confidentiality, dynamic update secrecy and significantly reduce computation overhead and the data uploading communication overhead. Zhang *and his colleagues* [55] address adoption of public cloud computing administrations incorporate administration unwavering quality, information security and protection, direction agreeable prerequisites and so on. The author proposing a hybrid cloud computing model which clients might acknowledge as a reasonable and cost-sparing strategy to make the best utilization of public cloud benefits alongside their exclusive (legacy) server farms. These exhibits the plan of a hybrid cloud computing model, it permits clients to build up another design where a committed asset stage keeps running for facilitating base administration workload, and a different and shared resource platform serves flash crowd peak load.

Yuchuan *and his colleagues* [56] proposed the Internet is a driving force towards the different advances that have been produced since its commencement. Apparently, the most talked about among every one of them is Cloud Computing. In the course of the most recent couple of years, distributed computing strategy has seen a huge move towards its appropriation and it has turned into a pattern in the data innovation space. It guarantees noteworthy cost decreases and new business potential to its clients and suppliers. The advantages of utilizing distributed computing include; i) Reduced equipment and support cost ii) Accessibility around the globes iii) Flexibility and profoundly computerized forms wherein the client require not stress over commonplace concerns like programming up-gradation. Bharath *and his colleagues* [57] observe that when the information proprietor denies a portion of the clients' get to rights there is an issue of potential productivity with the outsourced encoded information. The answer for this issue depends on symmetric key encryption strategy however it is not sheltered when a renounced client rejoins the framework with various privileges to similar information record. Proposed plan is an efficient and Secure Data Sharing (SDS) structure utilizing intermediary re-encryption and homomorphic encryption schemes that avoid a strategic distance from the spillage of unlawful information when a denied client rejoins the framework. J

iaxin *and his colleagues* [58] exploiting propose a layered progressive resource allocation algorithm for multi-tenant cloud server farms in view of the Multiple Knapsack Problem (LP-MKP). The LP-MKP calculation utilizes a multi-organize layered dynamic technique for multi-inhabitant VM distribution and proficiently handles natural occupants at each stage. This diminishes asset discontinuity in cloud server farms, diminishes the distinctions in the QoS among occupants and enhances inhabitants' general QoS in cloud server farms. Duan *and his colleagues* [59] considered how to concurrently afford maximum performance non-blocking multicast virtual systems and lessen equipment cost in fat-tree server farm systems, in order to plot virtual systems to physical foundation efficiently, they had made cautious choices on the allocation of inadequate resources, which makes placement of virtual networks in data centers a critical issue. The placement of virtual networks in fat-tree server farm systems is considered. In order to assemble the necessities of immediate parallel information exchange between various computing units, proposed a model of Multicast Capable Virtual Networks (MVNs), then design four Virtual Machine (VM) assignment plans to embed MVNs into fat-tree data center networks, called Most-Compact-First (MCF), Most Vacant Fit (MVF) and Mixed Bidirectional Fill (MBF) and Malleable Shallow Fill (MSF). Li *and his colleagues* [60] introduced more useful algorithms for foreseeing the consummation times of game sessions by studying the issue of how to transmit the play solicitations to the cloud servers in a cloud gaming framework. They demonstrate that the dispatching methodology of play solicitations may greatly involve the aggregate administration cost of the cloud gaming framework. The play request dispatching issue can be considered as an alternative to the dynamic bin packing issue. This scheme allocates play asks for according to the anticipated completion times of diversion sessions. The decrease in the asset waste is mainly considerable for match-based games. Raghavendra *and his colleagues* [61] focus on reducing search time on encrypted data set by constructing the Domain and Range Specific Index Generation (DRSIG) conspire which restricts the index generation period, for accomplishing compelling information use through the Internet over remotely put away encoded cloud information. A scientific model is utilized which encodes the recorded watchword that expels the spillage of data. It is watched that DRSIG plan is extremely productive and gives a more secure method for information recovered than Ranked Searchable Symmetric Encryption (RSSE) scheme. Swarupkshatriya *and his colleagues* [62] developed to achieve the requirements like Data security, Privacy, Information secrecy and Fine-grained access control, resources are recovered from the web through online devices and applications, rather than direct. In this technology users have to trust their information to cloud suppliers, there are a few security and protection worries on outsourced information.

Qinlong *and his colleagues* [63] discusses the novel Digital Rights Management (DRM) schemes experience from wastefulness and can't bolster dynamic upgrading of use rights put away in the cloud. The author proposes a novel DRM plot with safe key management and element use control in cloud computing and present a safe key administration instrument in light of characteristic based encryption and intermediary re-encryption. Just the clients whose characteristics fulfill the get to the arrangement of the scrambled substance and who have viable utilization rights can have the capacity to recuperate the substance encryption key and further decode the content. Elham *and his colleagues* [64] highlighted the different techniques of information segregation in the distributed computing environments to improve data security and towards the quick development of cloud computing is the security, since the data and information are the backbones of any organization. Their aim is to discuss data segregation technique to enhance data security cloud computing and also describes the advantages and disadvantage of the existing data segregation strategies and techniques. Many researchers proposed models for data protection and to enhance data security such as data segregation techniques. Cui *and his colleagues* [65] focus on the challenge to plan in which encryption plans lies in the proficient administration of encryption keys. The preferred adaptability of disseminating any cluster of chose records with any cluster of client's requests for various reports, different encryption keys to be utilized. Proposing the novel considered Key Aggregate Searchable Encryption (KASE) conspire, in which an information proprietor basically needs to share out a solitary key to a client for sharing an expansive number of archives and the client just needs to introduce a solitary access with the cloud for questioning the common reports. This plans are secure and for all intents and purposes effective.

Ray *and his colleagues* [66] presented semi-trusted cloud providers. To resolve Service Level Agreements (SLA), used has encryption approaches like ABE, key-policy attribute based, ciphertext policy based etc. Rong *and his colleagues* [67] observe that task assignment and capability of proficient scheduling in a shared MapReduce environment is a challenging task in Hadoop. The conventional scheduling algorithms supported by Hadoop will always not assure good average response times under diverse workloads. To address this problem by introducing a novel Hadoop scheduler, which deliberates the knowledge of patterns of workload to reduce average job response times and using Workload Pattern Based Scheduler (WPBS) technique of adaptive scheduling for improving the efficiency of Hadoop systems which process diverse Map Reduce jobs. Xia *and his colleagues* [68] demonstrate the designing of a searchable dynamic encryption format which updates operation and it can be finished by cloud server only, temporarily keeping the capacity to bolster multi-keyword ranked search. Projected scheme generally considers the challenge from the cloud server. A protected, dynamic and efficient search technique is proposed, which underpins the dynamic cancellation and addition of reports. They make an uncommon watchword adjusted parallel tree as the file, and propose a ”Greedy Depth First Search” algorithm to increase upgraded effectiveness than linear search. Zhang *and his colleagues* [69] noticed the issue of secure fuzzy keyword look in a multi-proprietor worldview to empower cloud servers to evaluate secure pursuit without knowing the genuine information of both keyword and trapdoors. Deliberately constructed a new protected pursuit rules. To avoid the aggressors from secret keys and putting on a show to be legitimate information clients submitting looks, a novel element mystery key era convention and another information client confirmation protocol developed and furthermore explored the issue of secure multi-keyword scan for numerous information proprietors.

Raghavendra *and his colleagues* [70] focused on minimizing the computation overhead, cost of information on owner side and the time complexity of search time. Most Significant Single keyword Search (MSSS) that backings efficient inquiry over encrypted cloud information in which it uses a Most Significant Digit (MSD) radix sort. MSD radix sort algorithm sorts the keyword in record document and counting sort algorithm is utilized to group up the keywords that are having same ASCII esteem into a pail. MSSS algorithm is performed on the genuine informational collection that shows lessening in record storage space, index generation time and keyword search time. Singh *and his colleagues* [71] introduced the concept of Proxy signature and proxy re-encryption are used. A Digital Envelope (DE) is a sheltered electronic information holder that is used to provide security to a message receivable to encryption and information verification. The DE permits consumers to encrypt their information by means of high speediness of secret-key encryption and the convenience and public key encryption security. The information is encrypted by an erratically chosen session key. The utilization of public-key encryption based on the chosen session key is encrypted using the public key of particular consumer [72,73,74].

Nabeel *and his colleagues* [75] addressed a novel key management method, named Broadcast Group Key Management (BGKM) then a safe development of a BGKM plan called ACVBGKM. An imperative issue out in the open cloud is the manner by which to specifically share records in view of fine grained attribute based Access Control Policies (ACPS). A methodology is to encode reports fulfilling distinctive strategies with various keys utilizing an open key cryptosystem, for example, attribute-based encryption as well as proxy re-encryption. A key advantage of the BGKM plan is that including clients/denying clients or refreshing ACPS can be performed proficiently by upgrading just some open data. In [76], many people use trivial passwords which easy to guess or they collect the passwords and some notes from the computer. It is done by clever (wise) hackers by writing keystroke logging programs. These programs stores the all keys including all passwords client entered. So they make sure that the logging person must and should enter the unforgeable password, which is effective only one time and variations each interval client sign-in. This is known as One-Time Password (OTP). It might be sent to your cell phone (the number is given at the time of register) as an SMS text message. By this, the security is enhanced in sharing data. Any member of a group can leave whenever they want except group leader. If group leaves, the group will be collapsed.

5.4 Social cloud computing

It is a shared social distributed computing. In cloud computing to incorporate the sharing, bargaining, and leasing of computing resources across over associates whose proprietors and administrators are checked through a social network or reputation system. Chard *and his colleagues* [77] studied the online relationships in social networks that are frequently in view of genuine connections to be utilized for inferring a level of trust between clients. The proposed utilizing these connections to frame dynamic "Social Cloud", consequently empowering clients to share varied assets inside the setting of social community. Furthermore, the intrinsic socially restorative mechanisms (motivations) can be utilized to empower a cloud-based system for long haul offering to lower protection concerns and security overheads are available in conventional cloud situations. Because of the novel way of the Social Cloud, a social commercial place is a method for managed sharing. The social market is novel, as it customs both social and financial conventions to encourage exchanging. This is characterized Social Cloud computing, laying out different parts of Social Clouds and shows the approach utilizing a social storage cloud usage in Facebook.

Surjimol [78] observes the main issues like provider certification and service level agreements of trust and accountability and providing their sharing preferences, by using clustering based on relationship lists and relationship strength methods which automatically identify them from their social network. This methodology, the architecture, and design of a Social compute cloud, a combination of Cloud Computing, Volunteer Computing, and the Social network has been deployed. In addition, it is used by clients to communicate with each other and interact with the resources of their friends. A client-centric methodology to authentication for household networks is recommended. Liu *and his colleagues* [79] anticipated a Shared Authority based Privacy preserving Authentication protocol (SAPA) to address privacy problem for cloud storage. The author explains a Zero Knowledge Proof (ZKP) authentication. This is used to control the emerging cloud arrangement allowing users to momentarily transfer their facility and content rights inside a trusted atmosphere such as a friend's home. This attitude enables the distribution of personalized content and more erudite network based facilities over a conservative TCP/IP infrastructure.

5.5 Framework

The framework is used as accumulations of anything from development tools to middleware to database benefits that facilitate the creation, sending and administration of cloud applications. Tsoutsos *and his colleagues* [80] introduced a new based secure group sharing hidden outline for an open cloud, it successfully takes the benefit of the cloud server's assistance yet have no delicate information or data being presented to assailants and to the cloud supplier. This scheme joins strategies like a proxy signature, Improved TGDH and intermediary re-encryption composed into a procedure. Utilizing the proxy signature procedure, the group leader can progressively give the benefit of group administration to at least one picked among the people. The Improved TGDH technique helps the group to arrange and update the group key sets with the help of cloud servers, which does not require the greater part of the group individuals been online constantly. The CloudSched empowers procedures demonstrating and recreation of Cloud server farms, particularly distributing virtual machines to proper physical machines. CloudShed can deal with an expansive number of Cloud server farms, comprising of many physical machines. Diverse scheduling algorithms are utilized as a part of various data centers based on of clients' necessities [81].

5.6 Data security

Security is the set of control-based innovations and strategies intended to cling to administrative consistency runs and ensure data, information applications, and framework related to distributed computing. A Key-Policy Attribute-Based encryption by Time Specified Attributes (KP-TSABE), is a new type information protected self-destructing plan in distributed computing. In the KP-TSABE technique, each ciphertext is assigned by a period interim though the secretive key is connected with a period moment [82,83,84]. If both the time moment is in the permitted time interim and the traits associated with the ciphertext satisfy the key's access to erection then the ciphertext can be decoded. The different methods in KPTSABE are as follows; i) Confidentiality of data and integrity, ii) Access control, iii) Sharing of data (forwarding) without utilization process sensitive re-encryption, iv)Security and v) Forward and backward access control. There are different techniques that are given for analyzing the reliability and checking the errors prediction in machines. Cloud Based Reasoning (CBR) method which predicts error in the machine is adopted, as it has been commonly used worldwide even when cloud-based solution is applied on other error prediction approach. When there is a new problem based on past experience used CBR to find a solution. These experiences are organized in case of base with respect to processes involved in the CBR are; i) Retrieving same cases from the case base, ii) Reusing the data or information in the retrieved cases, iii) Regenerating the solution and iv) Retaining a new experience into the case base.

Lin *and his colleagues* [85] explained Homomorphic encryption and Proxy re-encryption techniques prevents the leakage of unauthorized information while revoked user re-joins the group and modified the underlying SDS infrastructure and exhibits a new solution based on the data between a revoked user. While concentrating on the different information proprietor scenario, divide the clients in the group into a few security areas that effectively reduce the key services difficulty for proprietors and customers. A maximum level of patient security is guaranteed by misusing Hierarchical, Multi-Authority Attribute Sets Based Encryption (HM-ASBE) and Advanced Encryption Standard (AES). Dong *and his colleagues* [86] optimizes the heterogeneous proxy re-encryption algorithm and recover the efficiency of encryption by sinking the overhead due to the interaction between involved parties. The author proposed a systematic skeleton of sharing secure sensitive data on big data platform, which ensure secure storage and submission of sensitive data based on the algorithm and guarantees usage of secure clear text in the cloud platform. In the meantime, information proprietors protect complete control of their own information in a domain.

Wang *and his colleagues* [87] proposed the concept of robustly handle with expansive scale information and along these support clients to accept distributed storage services more assertively with securely set up an effective Third Party Auditor (TPA). The evaluating procedure ought to fetch in no new susceptibilities near client information security. Proposed scheme secures cloud storage framework by supporting security protecting open auditing, utilizes the homomorphic direct authenticator and subjective veiling to guarantee that the TPA would not increase any data about the information content put away on the cloud server. Performance analysis and extensive security demonstrate the plans are secure and exceedingly proficient [88]. Ye *and his colleagues* [89] facilitate resource sharing and client's tasks are restricted for generation of certification key and strategy keys by the scheme which permits cloud clients to deliberate their access authorizations to different clients so effectively. Utilizing the policies of access control which monitor the entrance to accreditations and the assets put together by customers, an outsider can accumulate data on the cloud clients. To ensure the classification of the information stored lying on cloud provider's data encoder is used. This plan is more elastic, simple to utilize, efficient and flexible. Son *and his colleagues* [90] introduced the concept of secure cloud Digital Video Recorder (DVR) infrastructure based on individual virtualization to securely afford various functions through cloud resources. The architecture uses an Input/output Management Unit (IOMMU), this unit serves as Direct Memory Access (DMA) remapping for constructing secure personal virtualization. Yu *and his colleagues* [91] concentrate on addressing privacy of the data issues using Searchable Symmetric Encryption (SSE). In the cloud, one can take the file which client is interested. This can be achieved by secure multiword top-k retrieval. A series of symmetric encryption is applied. The Boolean keyword is also allowed here in this scheme.

5.7 Resource allocation

Resource assignment is the path toward apportioning and directing assets in a way that sponsorships and affiliation's key targets. Alasaad and his colleagues [92] proposed an algorithm for resource reservation that maximally reduces promotional charges accessible in the tariffs, while guaranteeing that adequate assets are held in the cloud. Circulated figuring offers a flexible system that media content providers can use to obtain storing assets that match the demand. For this circumstance, an open issue is to pick both the suitable measure of assets saved in the cloud. These reservation time with the end goal that the budgetary cost of the media content provider is decreased. Prediction Based Resource Allocation algorithm (PBRA) that diminishes the monetary cost of asset reservation in the cloud by maximally abusing marked down rates offered in the taxes, while ensuring that sufficient assets are held in the cloud with some level of confidence in probabilistic sense.

Xiong *and his colleagues* [93] presented a Key-Policy Attribute-Based Encryption with Time Specified attributes (KP-TSABE). A novel ensured data self-destructing arrangement in conveyed registering. It is unreasonable to execute full lifecycle insurance security, get to control transforms into a testing errand, especially to share fragile data on cloud servers. KP-TSABE plan, each ciphertext is set apart with a period between times while private key is connected with a period moment. The ciphertext must be decoded if both the time minute is in the allowed time between time and the properties related with the ciphertext satisfy the key's get to structure. The KPTSABE can settle some key security issues by supporting customer described endorsement period and by giving fine grained get to control in the midst of the period [94].

Di *and his colleagues* [95] introduced the concept of optimized cloud framework execution in view of refined resource allotment, in processing client demands with composite services. The different plans to optimize resource allotment are; (i) A virtual machine resource allotment plan with a decreased processing overhead for task execution. (ii) The most appropriate task scheduling strategy with various design parameters. (iii) The most appropriate resource sharing plan to balanced distinct asset divisions on running tasks to the extent Proportional-Share Model (PSM), which can be divided into Absolute Mode (called AAPSM) and relative mode (RAPSM).

Lightest Workload First (LWF) reduce the overall Response Extension Ratio (RER) for both successive mode tasks and parallel-mode tasks. In an aggressive circumstance with over responsibility of resource, the best one is consolidating LWF with both AAPSM and RAPSM. Kyle *and his colleagues* [96] depicts GridSpice, a versatile open source reenactment structure for demonstrating, outlining and planning of the keen framework. Matrix Spice recreations can be overseen through a Representational State Transfer (REST), Application Programming Interface (API) or through a Python library, allowing customers to run reenactments. It permits utilities, energy services suppliers, controllers, specialists, educators and understudies to take care of issues in the smart grid. This can't be decisively displayed by existing test systems either in light of scale or demonstrating limit. The system can run collected entertainments using separate circulation and transmission structure test systems, while including least overhead. Sinnen and Leonel [97] presented the idea of keeping up the physical equipment assets of a server. In this, few virtual machines under eccentric workload unsettling influence is a testing errand to robotize. This is on the grounds that, firstly such virtualized servers regularly need to give administrations to numerous virtual machines (i.e., various applications) with various execution targets. Besides, the workloads for these applications (VMs) may change extra minutes in a capricious manner, henceforth the ass*et al*lotment choices must be made productively.

Seo *and his colleagues* [98] introduces a mediated CertificateLess encryption plan without matching operations for safely sharing delicate data in the open clouds. Mediated CertificateLess Public Key Encryption (mCL-PKE) tackles the key escrow issue in personality based encryption and testament repudiation issue in open key cryptography. In any case, existing mCL-PKE plans are either wasteful due to the utilization of costly matching operations or helpless against partial decoding assaults. In mCL-PKE scheme to develop a viable answer for the issue of distribution delicate data in open clouds. The cloud is utilized as a protected stockpiling and a key era focus. Jia *and his colleagues* [99] presents an adaptive framework, Service Maximization Optimization (SMO), which is designed to enhance the Quality of Service (QoS) of the soft real-time multimedia applications in multimedia distributed computing. Minimum memory bandwidth is considered as the significant bottleneck in multimedia distributed computing for more virtual machines (VMs) of multimedia processing requiring high memory bandwidth simultaneously. Additionally, contending memory bandwidth among parallel running VMs leads to poor QoS of the multimedia applications, missing the deadlines of these soft real-time multimedia applications. Adaptive memory bandwidth control mechanism alters the memory access rates of all the parallel running VMs to ensure the QoS of the soft real-time multimedia applications. SMO significantly enhances the QoS of the soft real-time multimedia applications with an irrelevant penalty on framework.

Xue *and his colleagues* [100] innovate a novel secure group sharing system for open cloud. Which can successfully exploit the cloud server's help however no delicate information being presented to assailants and the cloud supplier. Protection and security of group sharing information have turned out to be two noteworthy issues. The cloud supplier can't be dealt with as a trusted outsider by virtue of its semi-confide in nature and along these lines the conventional security protection models can't be immediate summed up into cloud-based group sharing systems. The structure joins proxy signature, improved Tree Based Group Diffie Hellman (TGDH) and intermediary re-encryption together into a convention. The improved TGDH plan empowers the group to arrange and update the group key sets with the assistance of cloud servers, which does not require the majority of the gathering individuals been online constantly. Embracing proxy re-encryption, greatest computationally serious operations can be assigned to cloud servers without uncovering any personal data. Lan Zhou *and his colleagues* [101] proposed a Role Based Encryption (RBE) conspire that incorporates the cryptographic methods with Role Based Access Control (RBAC). The quick improvements happening in distributed processing and benefits, there has been a developing pattern to utilize the cloud for vast scale information storage. This has increased the vital security problem of how to control and anticipate unapproved access to information stored in the cloud. To understand access control model, RBAC which gives adaptable controls and administration by having two mappings, clients to roles and roles to benefits on information objects. RBE conspire permits RBAC approaches to be enforced for the encoded information stored in open clouds. A protected RBE based hybrid distributed storage architecture allows a relationship to store data securely in an open cloud, while keeping up the sensitive information related to the association's structure in a private cloud. Raghavendra *and his colleagues* [102] proposed the Domain and Range Specific Index Generation (DRSIG) conspire that decreases the Index Generation time. The confidential information is encoded before transferring to the cloud server in order to protection and security. All conventional Searchable Symmetric Encryption (SSE) plans empower the clients to look for in general record. DRSIG method is productive and give more safe information than Ranked Searchable Symmetric Encryption (RSSE) method.

Zhu and Jiang [103] proposed a safe information sharing scheme for dynamic individuals. The regular variation of the participation, sharing information however giving security protecting is so far a testing issue, especially for an untrusted cloud as a result of the arrangement ambush. To give the protection, a protected route for key scattering with no sheltered correspondence channels and the customers can securely gain their private keys from group chief. Moreover, this arrangement can achieve fine-grained get to control, any customer in the group can use the source in the cloud and denied customers can't access the cloud once more. Secure the plan from conspiracy assault, which implies that denied clients can't get the original information document irrespective of the likelihood that they conspire with the untrusted cloud. At last, this scheme can accomplish fine efficiency, which implies past clients require not to update their secretive keys for the circumstance also another customer participates in the group or a customer is repudiated from the group.

Chow *and his colleagues* [104] concentrate unidirectional Proxy Re-Encryption (PRE), which the re-encryption key only empowers delegation in one direction however not the inverse, then proposed an efficient unidirectional PRE scheme. The proxy only needs a re-encryption key and can't learn anything about the plaintext encoded. This includes flexibility in different applications, for example, confidential email, digital right management and distributed storage. Shuanbao and Jianming [105] apply Broadcast Ciphertext Policy Attribute Based Encryption (CP-ABE) and attribute segmentation to manage this issue and perform solid development to accomplish scalable client revocation. Client revocation is the most trouble in cloud which revocation of any single client would influence other people who share regular attribute space. Communicate CP-ABE is a direct revocation architecture, fine-grained revocation should be possible without influencing any non-revoked clients. Attribute segmentation chooses whether to momentarily revoke client approval as per attribute subset. Liu *and his colleagues* [106] projected a novel open auditing strategy named Multi-Replica Dynamic Public Auditing (MuR-DPA). Nevertheless, existing information auditing methods experiences productivity and security issues. MuR-DPA scheme fused a novel Authenticated Data Structure (ADS) in a view of the Merkle Hash Tree (MHT), named as MR-MHT. In order to enhance information dependability and accessibility, storing various imitations alongside unique datasets is a typical procedure for cloud provision suppliers. Open information auditing plans permit clients to check their outsourced information storage without retrieving the entire dataset. To bolster (or support) full dynamic information updates and verification of piece indices. Chang *and his colleagues* [107] deliver a formal investigation to conceivable sorts of fine-grained information updates and suggest a plan that can completely bolster approved inspecting and fine-grained update demands. Distributed computing releases novel period in IT as it can deliver different flexible and accessible IT benefits in pay-as-you-go mold, wherever its clients be able to decrease the enormous assets interests in their personal IT foundation. Each little upgrade will bring about re-computation and informing of the authenticator for a whole document piece, which thus causes higher capacity and correspondence overheads. Further, enhanced that can drastically diminish communication overheads for checking little updates.

Qiang *and his colleagues* [108] introduce security model for a safe and scalable Multi-Party Searchable Encryption (MPSE) by considering the worst-case and average case scenarios, which capture different server-client collusion possibilities. The possibility that the cloud server may collude with some malicious clients, it is a challenge to have a safe and MPSE scheme. This is appeared by an analysis on the Popa Zeldovich scheme, which says that a legit client may leak all hunt search patterns of the possibility that shares only a single of reports to another malicious client.

5.8 Privacy and Dynamic

To secure private data is more challenging in cloud computing. The file owner share file's to authorize members. Jung *and his colleagues* [109], show a semi-anonymous privilege control plan, AnonyControl to address not just the information assurance, the customer personality security in present access control plans. The data substance protection and the access mechanism, while less thought is paid to the banquet control and the personality security. The AnonyControl-F, which totally keeps the identity leakage and finish the full anonymity [110]. Wang *and his colleagues* [111] proposed a safe cloud storage framework supporting protection assurance open auditing. In this manner, empowering open auditability for distributed storage is of basic significance that clients can turn to a Third Party Auditor (TPA) to check the uprightness of outsourced information and be effortless. Clients ought to have the ability to fair utilize the distributed storage as though it is local, without stressing the need to affirm its trustworthiness. Broad security and execution investigation demonstrate the proposed plans are provably secure and exceptionally effective.

Qia *and his colleagues* [112] identify a distributed computing application scenario that requires at the same time performing secure watermark location and preserving multimedia information storage. The author proposed a Compressive Sensing (CS) based structure utilizing secure Multi-Party Computation (MPC) protocols to address such a requirement. The multimedia information and secret watermark pattern are exhibited to the cloud for secure watermark discovery in a CS area to ensure the protection. In this framework extended to other collaborative secure signal processing and data-mining applications in the cloud. Rosa *and his colleagues* [113] proposed a security upgraded and trust aware Identity Management (IdM) architecture consistence with SAMLv2/ID-FF guidelines. The aim is to provide an efficient identity management, access control, a dynamic, autonomic and client driven framework for better versatility in distributed computing services. As to security, engages clients to access cloud services and share digital content without fundamentally uncovering their actual identity to everybody. The utilization of numerous identities, for instance, depending on the context. It provides a framework that empowers to keep to a follow off between client's protection and degree of tracking to get a satisfactory personalization degree in the distinctive services. Chen and Lee [114] concentrate the issue of remotely checking the trustworthiness of recovering coded information against defilements under a genuinely distributed storage setting. The creator, outline and execute a useful Data Integrity Protection (DIP) plan for a particular recovering code, while safeguarding its characteristic properties of adaptation to internal failure and repair-traffic saving. DIP plan is composed under a mobile Byzantine adversarial model and empowers a customer to possibly confirm the trustworthiness of arbitrary subgroups of outsourced information against general or malevolent debasements. A DIP plot for the FMSR codes under a multi-server setting. Functional Minimum Storage Regenerating (FMSR)-DIP codes, save the adaptation to internal failure and repair traffic saving properties of FMSR codes.

Xu *and his colleagues* [115] propose iAware, a lightweight obstruction mindful VM relocation methodology. To stay away from potential violations of Service Level Agreement (SLA) requested by cloud applications. It experimentally catches the fundamental connections between VM execution obstruction and key components that are for all intents and purposes open through sensible tests of benchmark workloads on a Xen virtualized group stage. Mindful mutually evaluates and reduces both movement and co-area obstruction among VMs, by planning a straightforward multi-asset request supply model. Tysowski and Hasan [116] presented the convention has been acknowledged on monetarily prevalent portable and cloud stages to exhibit genuine benchmarks that show the sufficiency of the plan. Delicate information stored in the cloud must be protected from being perused free by a cloud provider that is straightforward however inquisitive. Cloud-based data are continuously being accessed by asset constrained phones for which the taking care of and correspondence cost must be lessened. Novel adjustments to characteristic based encryption are proposed to allow endorsed customers access to cloud data in perspective of the satisfaction of obliged ascribes to such a degree, to the point that the higher computational load from cryptographic operations is appointed to the cloud provider and the aggregate correspondence cost is brought down for the portable customer. Data re-encryption performed by the cloud provider to decrease the cost of customer repudiation in a portable customer condition while protecting the security of client information stored in the cloud.

Renjith and Sabitha [117] proposed security concerns access be distinctly important as outsourcing the storage of possibly sensitive information to outsider distributed storage. Information stored in the cloud might be unexpectedly disclosed later on because of malicious assaults on the cloud or thoughtless management of cloud operators. Secure information exchange is expected to keep up the information security between approved clients. The challenge of accomplishing secure information sharing is to encrypt the information and in the meantime, it is available to those approved customers. The re-encryption process converts the ciphertext encoded under the public key to a different cipher text encrypted under the intended receiver's public key. The cloud rectifies the faithfulness of the clients without knowing the operators identify before loading information. The scheme additionally incorporates the feature like access control, in which solitary approved clients are capable of decoding the stored records. Public-key cryptosystems contrivance produce a fix-sized cipher text such that effective delegation of decryption privileges for any set of cipher texts are conceivable. A safe multi-owner information scrambling scheme for element sets in the cloud talk about the sharing of information upon the group [119]. By utilizing get together signature and element demonstrate encryption strategies, any cloud customer can secretly impart data to others. Heng *and his colleagues* [120] proposed a safe, proficient and fine-grained information Access Control component for P2P storage Cloud named ACPC. Cloud severs and clients are usually outside the trusted domain of information proprietors, P2P storage cloud delivers new difficulties for information security and access control when information proprietors store delicate information for sharing in the trustworthy domain. To address this issue, a ciphertext strategy Attribute Based Encryption (ABE) plot and a proxy re-encryption scheme. ACPC empowers information proprietors to ambassador most of the laborious client revocation tasks to cloud servers and respectable framework peers.

Mohammed *and his colleagues* [121] projected a two-party algorithm that discharges differentially private information secure path according to the description of safe multiparty computation. The privacy-preserving information distributing addresses the issue of revealing delicate information when digging for valuable data. This address the issue of the secretive information distributing, wherever diverse attributes for a similar set of people are held by twofold gatherings. Specifically, an algorithm for differentially secretive information discharge for vertically divided information among two gatherings in the semi-honest rival model. To accomplish this, a two-party convention for the exponential system. Any algorithm that having the exponential system in a disseminated settings. This convention can be used with sub-protocol.

Raja *and his colleagues* [122] introduce a novel structure, CloudView, for storage, preparing and analysis of gigantic machine support information, gathered from a huge number of sensors embedded in mechanical machines, in a distributed processing condition. The author proposed system use the parallel computing ability of a computing cloud on a huge scale dispersed clump preparing framework that is worked on item equipment. A Case-Based Reasoning (CBR) approach is embraced for machine fault forecast, where the past instances of disappointment from countless are accumulated in a cloud. The utilization of the cloud design for maintenance information storage, processing, analysis and assesses a few conceivable cloud-based models that use the benefits of the parallel processing capacities to settle on neighborhood choices with worldwide data effectively while keeping away from potential information bottlenecks that can happen in getting the support information all through the cloud. Rahulamathavan *and his colleagues* [123] proposed client-server information classification protocol utilizing support vector machine. Privacy Preserving (PP) information classification strategy where the server can’t take in any learning about customers’ information data tests while the server side classifier is kept mystery from the customers amid the classification procedure. In the cloud, information classification to be performed by conceivably untrusted servers. Inside, specific circumstance classifier constructed by the server can be used by customers so as to classify their private information samples in the cloud. The protocol accomplishes PP classification together two-party and multi-class issues. The convention misuses assets of pillar homomorphic encryption and protected two-party calculation. At the center of the convention deceits, an effective, new convention for securely getting the sign of pillar encoded numerals.

Li *and his colleagues* [124] proposed Dekey, a new improvement in which customers don’t need to manage any keys in solitude yet rather securely disperse the concurrent key shares over various servers. Promising as it is by all accounts, a developing test is to achieve secure deduplication in appropriated storage. In united encryption has been broadly gotten for secure deduplication, an essential issue of making concurrent encryption pragmatic is to effectively and dependably manage number of joined keys. A standard approach in which each customer holds a free master key for encoding the blended keys and outsourcing them to the cloud. A benchmark key organization plot creates a colossal number of keys with the growing number of customers and obliges customers to dedicatedly secure the master keys. Jin *and his colleagues* [125] proposed distributed deduplication frameworks with higher dependability quality in which the information pieces are conveyed over numerous cloud servers. Deduplication framework enhances storage usage while diminishing unwavering quality. The test of security for fragile data rises when they are outsourced by customers to cloud. Hoping to address the above security difficulties, to formalize the idea of distributed reliable deduplication framework. The security prerequisites of information classification and label consistency are additionally accomplished by presenting a deterministic mystery sharing plan in scattered stockpiling frameworks, rather than utilizing merged encoded as in past deduplication frameworks.

Okamoto and Takashima [126] demonstrate two Non-zero Inner Product Encryption (NIPE) plans that are adaptively secure under a standard presumption, the Decisional LINear (DLIN) suspicion, in the standard model. Any past Identity Based Revocation (IBR) plan with consistent size ciphertexts or consistent size secret keys were not adaptively safe in the standard model. NIPE plans highlight consistent size ciphertexts and alternate features consistent size private keys. NIPE plans suggest an IBR framework with consistent dimensions ciphertexts or consistent magnitude of private keys that is adaptively safe under the DLIN assumption. Wang *and his colleagues* [127] introduced a novel series derivation function for similar attribute-based encryption. An efficient structure called Constant size Ciphertext-Policy Comparative Attribute-Based Encryption (CCP-CABE) with the provision of adverse qualities/trump cards. CCP-CABE accomplishes the effectiveness since it creates consistent dimensions keys and ciphertext paying little mind to the quantity of included properties and it keeps the reckoning charge unfaltering on lightweight phones. CCP-CABE kept the computational upstairs consistent for the information proprietors and information clients paying little respect to the quantity of included attributes by scrambling and unscrambling overall traits in a batch-processing way. This keeps the correspondence upstairs little and relentless paying little respect to the quantity of characteristics. ECCP-CABE empowers the admittance strategy to organize the benefit stages of various property areas and ensures the strategy introduction space by space to ensure the protection of access to approach.

5.9 Load balancing

Cloud load balancing is the process of distributing workloads and computing resources in a cloud computing environment. This allows enterprises to manage application or workload demands by allocating resources among multiple computers, networks or servers. Guo *and his colleagues* [128] introduced the concept of load balancing processes. Hybrid resource management environs, working on both application and framework levels created for diminishing the execution time of parallel requests with the distinguishable task on heterogeneous Grid assets. The framework relies on upon the Adaptive Workload Balancing Algorithm (AWLB) fused into the Distributed Analysis Environment (DIANE), User Level Scheduling (ULS) Environment. Well, organized execution of parallel applications on heterogeneous and dynamic Grid resources is a more challenging problem that needs the development of adaptive workload balancing algorithms that would take application requirements and the resource features [129,130]. Wu [131] presents an overview of the parallel scheduling procedure. In parallel scheduling, all processors cooperate to schedule the work. It provides high-quality load balancing. Parallel scheduling is able to accurately balance the load by utilizing worldwide load data at compile-time or run-time. Parallel scheduling consolidates the advantages of static scheduling and dynamic scheduling.

Tian *and his colleagues* [132] present a lightweight Cloud assets planning emulator, CloudSched. There is still an absence of devices that empower designers to compare dissimilar resource scheduling algorithms in IaaS with respect to together processing servers and client jobs. Performance assessment of assignment models and Cloud provisioning algorithms in a repeatable way beneath various designs prerequisites is an issue. To overcome in tools for assessment and modeling of Cloud situations and applications. By using different resource scheduling algorithms, CloudSched can support designers to distinguish and investigate suitable. Dissimilar to conventional scheduling algorithms considering just a single component, that can bring about hotspots or bottlenecks by and large, CloudSched regards multidimensional resources like memory, CPU and network bandwidth incorporated for both physical machinery and virtual machinery for various scheduling objectives. Cloud Computing is the emerging technology, to provide data security is a major challenging task. To sharing of Private data is not secure in cloud environments. A study has been carried at the different concept in cloud technology such as privacy of data, sharing of files, load balancing and effective utilization of internal/external resources etc. Distributed environment we facing several issues such as Data privacy, Load balancing, Data sharing, energy efficiency, Deduplication, Regenerating code and Resource utilization. We focus on security for private/public data, Data sharing, Resource utilization, Load balancing and energy efficiency.

6. Conclusions

How to protect consumer’s private data in distributed cloud storage is challenging task. To share the personal file from one user to another user is most difficult using the cloud computing. To provide more secure to the data using different schemes. We studied different Cloud Computing concepts like mobile cloud computing, integrity and forward security, social cloud computing, framework, resource allocation, data security, privacy and dynamic, IOT and load balancing schemes. While concerning about the security of data we analyze different issues such as low security, high computational complexity, privacy/public file sharing and improper utilization of resources. There are distinctive scheduling strategies used in multiple federated data centers. Aggregate key provides more secure in sending file between sender and receiver. Forward security encryption and re-encryption techniques are used to provide high security for private data. It gives demonstrating and reproduction of substantial scale distributed computing, including data centers. Virtual Machines (VMs) and Physical Machines (PMs) consumes more power. This is the limitation, due to this, the cost of file transfer is increased. A further enhancement to overcome intruder’s attacks in private data, to provide more security and more sharing of files, effectively utilization of resources and reducing the energy consumption in VMs and PMs.

References

[1] Guillermo Indalecio, Fernando Gomez-Folgar, and Antonio J. GarciaLoureiro, “GWMEP: Task Manager-as-a-Service in Apache Cloud Stack”, IEEE Internet Computing, vol. 20, no. 2, pp. 42-49, March/April 2016.

[2] Lo, ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari, “A Secure Cloud Computing Model Based on Data Classification”, Elsevier Procedia Computer Science, vol. 52, pp. 1153-1158, 2015.

[3] Jean Bacon, David Eyers, Thomas F. J. M. Pasquier, Jatinder Singh, Ioannis Papagiannis and Peter Pietzuch, “Information Flow Control for Secure Cloud Computing”, IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 76-89, March 2014.

[4] Joseph K. Liu, Man Ho Au,Willy Susilo, Kaitai Liang, Rongxing Lu and Bala Srinivasan, “Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud”, IEEE Journal on Network, vol. 29, no. 2, pp. 46-50, 2015.

[5] Ming Li, Shucheng Yu, Yao Zheng, Kui Renand Wenjing Lou, ”Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, January 2013.

[6] LI Chaoling, CHEN Yue and ZHOU Yanzhou, “ADataAssuredDeletion Scheme in Cloud Storage”, IEEE China Communications, vol. 11, no. 4, pp. 98-110, April 2014.

[7] Mauro Gaggero and Luca Caviglione, “Predictive Control for EnergyAware Consolidation in Cloud Datacenters”, IEEE Transactions on Control Systems Technology, vol. 24, no. 2, pp. 461-474, 2016.

[8] Mahyar Movahed Nejad, Lena Mashayekhy and Daniel Grosu, “Truthful Greedy Mechanisms for Dynamic Virtual Machine Provisioning and Allocation in Clouds”, IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 594-603, 2015.

[9] Atta Ur Rehman Khan, Mazliza Othman and Sajjad Ahmad Madani, “Mobile Cloud Computing Application Models”, IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 393-413, 2014.

[10] Ki-Woong Park, Jaesun Han, JaeWoong Chung and Kyu Ho Park, “THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment”, IEEE Transactions on Services Computing, vol. 6, no. 3, pp. 300-313, July-September 2013.

[11] Sheng Di and Cho-Li Wang, “Error-Tolerant Resource Allocation and Payment Minimization for Cloud System”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1097-1106, June 2013.

[12] Elli Kartsakli, Angelos Antonopoulos, Aris S. Lalos, Stefano Tennina, Marco Di Renzo, Luis Alonso and Christos Verikoukis, “Reliable MAC Design for Ambient Assisted Living: Moving the Coordination to the Cloud”, IEEE Communications Magazine, vol. 53, no. 1, pp. 78-86, 2015.

[13] Jun Zhou, Xiaodong Lin, Xiaolei Dong and Zhenfu Cao, “PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System”, IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 6, pp. 1693-1703, June 2015.

[14] Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey and Jinjun Chen, “A Privacy Leakage Upper Bound Constraint-Based Approach for CostEffective Privacy Preserving of Intermediate Data Sets in Cloud”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1192-1202, June 2013.

[15] Joseph K. Liu, Man Ho Au and Xinyi Huang, “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services”, IEEE Transactions on Information Forensics and Security, vol. 11, no. 3,

pp. 484-497, March 2016.

[16] Haroon Raja and Waheed U. Bajwa, “Cloud K-SVD: A Collaborative Dictionary Learning Algorithm for Big, Distributed Data”, IEEE Transactions on Signal Processing, vol. 64, no. 1, pp. 173-188, 2016.

[17] Xuyun Zhang, Wanchun Dou and Jian Pei, “Proximity-Aware LocalRecoding Anonymization with MapReduce for Scalable Big Data Privacy Preservation in Cloud”, IEEE Transactions on Computers, vol. 64, no. 8, pp. 2293-2307, August 2015.

[18] Yong Yu, Yannan Li, Jianbing Ni, Guomin Yang, Yi Mu and Willy Susilo, “Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification”, IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 1717-1726, March 2016.

[19] TAN Shuang, TAN Lin, LI Xiaoling and JIA Yan, “An Efficient Method for Checking the Integrity of Data in the Cloud”, IEEE China Communications, vol. 11, no. 9, pp. 68-81, 2014.

[20] Yongdae Kim, Adrian Perrig and Gene Tsudik, “Group Key Agreement Efficient in Communication”, IEEE Transactions on Computers, vol. 53, no. 7, pp. 905-921, July 2004.

[21] Lazaros Gkatzikis and Iordanis Koutsopoulos, “Migrate or Not Exploiting Dynamic Task Migration in Mobile Cloud Computing Systems”, IEEE Wireless Communications, vol. 20, no. 3, pp. 24-32, 2013.

[22] S H Manjula, Bindu Reddy E, Shaila K, L Nalini, Venugopal K R and L M Patnaik, “Base-Station Controlled Clustering Scheme in Wireless Sensor Networks”, IFIP Wireless Days Conference, Dubai, e-ISBN: 978-1-4244-2829-8, p-ISBN: 978-1-4244-2828-1, pp. 1-5, November 24-27, 2008.

[23] Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong and Qi Xi, “A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”, IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, October 2014.

[24] 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, February 2014.

[25] Yuan Zhang, Chunxiang Xu, Shui Yu, Hongwei Li and Xiaojun Zhang, “SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems against Malicious Auditors”, IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159170, December 2015.

[26] Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[27] Anita Kanavalli, P Deepa Shenoy, Venugopal K R, L M Patnaik, A Flat Routing Protocol in Sensor Networks, International Conference on Methods and Models in Computer Science, New Delhi, ISBN: 978-14244-5051-0, pp. 1-5, December 1416, 2009.

[28] Kaitai Liang and Willy Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage”, IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1981-1992, September 2015.

[29] Kan Yang, Zhen Liu, Xiaohua Jia and Xuemin (Sherman) Shen, “TimeDomain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach”, IEEE A Cryptographic Approach, vol. 18, no. 5, pp. 940-950, 2016.

[30] Junbeom Hur, “Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 11, pp. 2171-2180, November 2013.

[31] S.S.M. Chow, Y. Dodis, Y. Rouselakis and B. Waters, “Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions”, Proceedings ACM Conference Computer and Comm. Security, pp. 152-161, 2010.

[32] T.H. Yuen, S.S.M. Chow, Y. Zhang and S.M. Yiu, “Identity-Based Encryption Resilient to Continual Auxiliary Leakage”, Springer Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 112-134, 2012.

[33] S Raghavendra, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar, and L M Patnaik, DRSMS: Domain and Range Specific MultiKeyword Search over Encrypted Cloud Data”, International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no. 5, pp. 69-78, May 2016.

[34] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, “Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 384-394, February 2014.

[35] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and Weixin Xie, “An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing”, IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265-1277, June 2016.

[36] Wenhai Sun, Bing Wang, Ning Cao, Ming Li, Wenjing Lou, Y. Thomas Hou and Hui Li, “Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025-3035, November 2014.

[37] Raghavendra, Girish S, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik, “IGSK: Index Generation on Split Keyword for Search over Cloud Data”, IEEE in Proceedings of CoCoNET 2015, Trivandrum, December 2015.

[38] Kan Yang and Xiaohua Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, September 2013.

[39] Olivier Beaumont, Lionel Eyraud-Dubois, Christopher Thraves Caro and Hejer Rejeb, “Heterogeneous Resource Allocation under Degree Constraints”, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 5, pp. 2354-2363, May 2013.

[40] Arshdeep Bahga and Vijay K. Madisetti, “Analyzing Massive Machine Maintenance Data in a Computing Cloud”, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1831-1843, October 2012.

[41] Sharrukh Zaman and Daniel Grosu, “A Combinatorial Auction-Based Mechanism for Dynamic VM Provisioning and Allocation in Clouds”, IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 129-141, July-December 2013.

[42] Kushang Parikh, Nagesh Hawanna, Haleema.P.K, Jayasubalakshmi.R and N.Ch.S.N.Iyengar, “Virtual Machine Allocation Policy in Cloud Computing Using CloudSim in Java”, International Journal of Grid Distribution Computing, vol. 8, no. 1, pp. 145-158, 12 2015.

[43] Song Wu, Zhou, Huahua Sun, Hai Jin and Xuanhua Shi, “Poris: A Scheduler for Parallel Soft Real-Time

Applications in Virtualized Environments", IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 3, pp. 841-854, 2016.

[44] Xiaolin LI, V. Bharadwaj and C. C. KO, "Divisible Load Scheduling on Single-Level Tree Networks with Buffer Constraints", IEEE Transactions on Aerospace and Electronic Systems, vol. 36, no. 4, pp. 1298-1308, October 2000.

[45] Zeng Zeng and Bharadwaj Veeravalli "Design and Performance Evaluation of Queue-and-Rate-Adjustment Dynamic Load-Balancing Policies for Distributed Networks", IEEE Transactions on Computers, vol. 55, no. 11, pp. 1410-1422, November 2006.

[46] Juan Du, Daniel J. Dean, Yongmin Tan, Xiaohui Gu and Ting Yu, "Scalable Distributed Service Integrity Attestation for Software-as-aService Clouds", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 730-739, March 2014.

[47] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE Transactions on Computers, vol. 64, no. 4, pp. 971-983, April 2015.

[48] P.Krithika, G.Linga Dilipan and M.Shobana, "Enhancing Cloud Computing Security for Data Sharing within Group Members", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 17, no. 2, pp. 110-114, Ver. V, MarApr. 2015.

[49] Aritra Dasgupta and Robert Kosara, "Adaptive Privacy-Preserving Visualization Using Parallel Coordinates", IEEE Transactions on Visualization and Computer Graphics, vol. 17, no. 12, pp. 2241-2248, December 2011.

[50] Chao-Yung Hsu, Chun-Shien Lu and Soo-Chang Pei, "Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT", IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4593-4607, November 2012.

[51] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, pp. 43-56, January-March 2014.

[52] B. Wang, S.S.M. Chow, M. Li and H. Li, "Storing Shared Data on the Cloud via Security-Mediator", IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), pp. 124-133, 2013.

[53] Jiawei Yuan and Shucheng Yu "Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification", IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, August 2015.

[54] Mi Wen, Kaoru Ota, He Li, Jingsheng Lei, Chunhua Gu and Zhou Su, "Secure Data Deduplication with Reliable Key Management for Dynamic Updates in CPSS", IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 137-147, December 2015.

[55] Hui Zhang, Guofei Jiang, Kenji Yoshihira and Haifeng Chen, "Proactive Workload Management in Hybrid Cloud Computing", IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 90-100, 2014.

[56] LUO Yuchuan, FU Shaojing, XU Ming and WANG Dongsheng, "Enable Data Dynamics for Algebraic Signatures Based Remote Data Possession Checking in the Cloud Storage", IEEE Communications, vol. 11, no. 11, pp. 114-124, 2014.

[57] Bharath K Shamanthula, Yousef Elmehdwi, Gerry Howser and Sanjay Madria, "A Secure Data Sharing

and Query Processing Framework via Federation of Cloud Computing", Elsevier Information System journal, vol. 48, pp. 196-212, 2015.

[58] Jiaxin, Dongsheng Li, Yuming Ye and Xicheng Lu, "Efficient MultiTenant Virtual Machine Allocation in Cloud Data Centers", Tsinghua Science and Technology, vol. 20, no. 1, pp. 81-89, 2015.

[59] Jun Duan and Yuanyuan Yang, "Placement and Performance Analysis of Virtual Multicast Networks in Fat-Tree Data Center Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 10, pp. 3013-3028, 2016.

[60] YusenLi,XueyanTangandWentongCai, "PlayRequestDispatchingfor Efficient Virtual Machine Usage in Cloud Gaming", IEEE Transactions on Circuits and Systems for Video Technology, vol. 25, no. 12, pp. 20522063, 2015.

[61] S Raghavendra, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik, DRSIG: Domain and Range Specific Index Generation for Encrypted Cloud Data", in Proceedings of International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016, March 11-13, 2016.

[62] Swarupkshatriya and Dr.Sandip M Chaware, "A Survey on Data Sharing Using Encryption Technique in Cloud Computing", International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, no. 4, pp. 5351-5354, 2014.

[63] Huang Ginlong, Ma Zhaofeng, Yang Yixian, Niuxinxin and Fujingyi, "Attribute Based DRM Scheme with Dynamic Usage Control in Cloud Computing", IEEE China Communications, vol. 11, no. 4, pp. 50-63, 2014.

[64] Elham Abd Al Latif A Badawi and Ahmed Kayed, "Survey on Enhancing the Data Security of the Cloud Computing Environment by Using Data Segregation Technique", Academic Research Publishing Agency:(arapapress) International Journal of Research and Reviews in Applied Sciences, vol. 23, no. 2, pp. 136, May 2015.

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

[66] Indrajit Ray, Kirill Belyaev, Mikhail Strizhov, Dieudonne Mulamba and Mariappan Rajaram, "Secure Logging As a Service-Delegating Log Management to the Cloud", IEEE Systems Journal, vol. 7, no. 2, pp. 323-334, June 2013.

[67] Rong Yu and Stein Gjessing, "Toward Cloud-Based Vehicular Networks with Efficient Resource Management", IEEE Network Journal, vol. 27, no. 5, pp. 48-55, 2013.

[68] Zhihua Xia, Xinhui Wang, Xingming Sun and Qian Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, February 2016.

[69] Wei Zhang, Yaping Lin, Sheng Xiao, Jie Wu and Siwang Zhou, "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing", IEEE Transactions on Computers, vol. 65, no. 5, pp. 1566-1577, May 2016.

[70] S Raghavendra, C M Geeta, K Shaila, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik, "MSSS: Most Significant Singlekeyword Search over Encrypted Cloud Data", International

Conference on ICT: Big Data, Cloud and Security, Singapore, Global Science and Technology Forum (GSFT), ISSN: 2251-3043, pp. 43-48, July 27-28, 2015.

[71] Rampal Singh, Sawan Kumar and Shani Kumar Agrahari, “Ensuring Data Storage Security in Cloud Computing”, IOSR Journal of Engineering, vol. 2, no. 12, pp. 17-21, December 2012.

[72] N. Shang, M. Nabeel, F. Paci and E. Bertino, “Preserving Policy-Based Content Sharing in Public Clouds”, IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2602-2614, 2013.

[73] 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.

[74] R. L. Grossman, “The Case for Cloud Computing”, IEEE IT Professional, vol. 11, no. 2, pp. 23-27, Mar-April 2009.

[75] Mohamed Nabeel, Ning Shang and Elisa Bertino, “Privacy Preserving Policy-Based Content Sharing in Public Clouds”, IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2602-2614, November 2013.

[76] http://searchsecurity.techtarget.com/definition/one-time-password-OTP.

[77] Kyle Chard, Kris Bubendorfer, Simon Caton and Omer F. Rana, “Social Cloud Computing: A Vision for Socially Motivated Resource Sharing”, IEEE Transactions on Services Computing, vol. 5, no. 4, pp. 551-563, October-December 2012.

[78] Surjimol R “A Social Compute Cloud: For Sharing Resources”, International Journal of Science and Research (IJSR), vol. 4, no. 2, February 2015.

[79] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, “Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing”, IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 241-251, 2015.

[80] Nektarios Georgios Tsoutsos and Michail Maniatakos, “The HEROIC Framework: Encrypted Computation without Shared Keys”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 6, pp. 875-888, June 2015.

[81] S Raghavendra, Doddabasappa P A, C M Geeta, Rajkumar Buyya, K R Venugopal, 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, 2016.

[82] Xiangming Dai, Jason Min Wang and Brahim Bensaou, “EnergyEfficient Virtual Machines Scheduling in Multi-Tenant Data Centers”, IEEE Transactions on Cloud Computing, vol. 4, no. 2, pp. 210-221, 2016.

[83] Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai, “Secure Auditing and Deduplicating Data in Cloud”, IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386-2396, August 2016.

[84] CHEN Danwei, CHEN Linling, FAN Xiaowei, HE Liwen, PAN Su and Hu Ruoxiang, “Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing”, IEEE Journal of China Communications, vol. 11, no. 13, pp. 121-127, 2014.

[85] Jenn-Wei Lin, Chien-Hung Chen and J. Morris Chang, “QoS-Aware Data Replication for Data-Intensive Applications in Cloud Computing Systems”, IEEE Transactions on Cloud Computing, vol. 1, no. 1, pp. 101-115, January-June 2013.

[86] Xinhua Dong, Ruixuan Li, Heng He, Wanwan Zhou, Zhengyuan Xue and Hao Wu, "Secure Sensitive Data Sharing on a Big Data Platform", IEEE Tsinghua Science and Technology, vol. 20, no. 1, pp 72-80, February 2015.

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

[88] S.S.M. Chow, Y.J. He, L.C.K. Hui and S.M. Yiu, "SPICE: Simple Privacy-Preserving Identity-Management for Cloud Environment", Springer Applied Cryptography and Network Security (ACNS), vol. 7341, no. 4, pp. 526-543, 2015.

[89] XinfengYe "PrivacyPreservingandDelegatedAccessControlforCloud Applications", IEEE Tsinghua Science and Technology, vol. 21, no. 1, pp. 40-54, February 2016.

[90] Junggab Son, Rasheed Hussain, Hunmin Kim and Heekuck Oh, "SCDVR: A Secure Cloud Computing Based Framework for DVR Service", IEEE Transactions on Consumer Electronics, vol. 60, no. 3, pp. 368-374, August 2014.

[91] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue and Minglu Li, "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239-250, July/August 2013.

[92] Amr Alasaad, Kaveh Shafiee, Hatim M. Behairy and Victor C.M. Leung, "Innovative Schemes for Resource Allocation in the Cloud for Media Streaming Applications", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 1021-1033, April 2015.

[93] Jinbo Xiong, Ximeng Liu and Zhiqiang Yao, "A Secure Data SelfDestructing Scheme in Cloud Computing", IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 448-458, October-December 2014.

[94] Jianfeng Ma, Qi Li, Kui Geng and Patrick S. Chen, "A Secure Data Self-Destructing Scheme in Cloud Computing", IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 448-458, October-December 2014.

[95] Sheng Di, Derrick Kondo and Cho-Li, "Optimization of Composite Cloud Service Processing with Virtual Machines", IEEE Transactions on Computers, vol. 64, no. 6, pp. 1717-1726, June 2015.

[96] Kyle Anderson, Jimmy Du, Amit Narayan and Abbas El Gamal, "GridSpice: A Distributed Simulation Platform for the Smart Grid", IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 23542363, November 2014.

[97] Oliver Sinnen and Leonel A. Sousa, "Communication Contention in Task Scheduling", IEEE Transactions on, Parallel and Distributed Systems, vol. 16, no. 6, pp. 503-515, June 2005.

[98] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-2119, September 2014.

[99] Gangyong Jia, Guangjie Han and Daqiang Zhang, "An Adaptive Framework for Improving Quality of Service in Industrial Systems, IEEE Access, vol. 3, pp. 2129-2139, 2015.

[100] 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.

[101] Lan Zhou, Vijay Varadharajan and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[102] Raghavendra, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik, “MSIGT: Most Significant Index Generation Technique for Cloud Environment”, IEEE International Conference, INDICON 2015, New Delhi, December 17-20, 2015.

[103] Zhonmga Zhu and Rui Jiang, “A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud”, IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 40-50, January 2016.

[104] S.S.M. Chow, J. Weng, Y. Yang and R.H. Deng, “Efficient Unidirectional Proxy Re-Encryption”, Springer International Conference on Cryptology in Africa, pp. 316-332, July 2010.

[105] LI Shuanbao and FU Jianming, “User Revocation for Data Sharing Based on Broadcast CP-ABE in Cloud Computing”, IET Communications Security Conference (CSC 2014), 2014, pp. 1-8, 2014.

[106] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang and Jinjun Chen, “MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud”, IEEE Transactions on Computers, vol. 64, no. 9, pp. 26092622, September 2015.

[107] Chang Liu, Jinjun Chen, Laurence T. Yang, Xuyun Zhang, Chi Yang, Rajiv Ranjan and Ramamohanarao Kotagiri, “Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2234-2244, September 2014.

[108] Qiang Tang, “Nothing is for Free: Security in Searching Shared and Encrypted Data”, IEEE Transactions on Information Forensics and Security, vol. 9, no. 11, pp. 1943-1952, November 2014.

[109] Taeho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan, “Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption”, IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 190-199, January 2015.

[110] Tanuja R, Shruthi Y R, Manjula S H, Venugopal K R and L M Patnaik, “Token based Privacy Preserving Access Control in Wireless Sensor Networks”, In Proceedings of IEEE 21st Annual International Conference on Advanced Computing and Communications ADCOM2015, IIT Chennai, pp. 45-50, 2015.

[111] C. Wang, S.S.M. Chow, Q. Wang, K. Ren and W. Lou “PrivacyPreserving Public Auditing for Secure Cloud Storage”, IEEE Transaction of Computers, vol. 62, no. 2, pp. 362-375, February 2013.

[112] Qia Wang, Wenjun Zeng and Jun Tian, “A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework”, IEEE Transactions on Image Processing, vol. 23, no. 3, pp. 1317-1328, March 2014.

[113] Rosa Snchez, Florina Almenares and Patricia Arias, “Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing”, IEEE Transaction on Consumer Electronics, vol. 58, no. 1, pp. 98-103, 2012.

[114] Henry C.H. Chen and Patrick P.C. Lee, “Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 407-416, February 2014.

[115] Fei Xu, Fangming Liu, Linghui Liu, Hai Jin, Bo Li and Baochun Li, "iAware: Making Live Migration of Virtual Machines InterferenceAware in the Cloud" , IEEE Transactions on Computers, vol. 63, no. 12, pp. 3012-3025, December 2014.

[116] Piotr K. Tysowski and M. Anwarul Hasan, "Hybrid Attribute and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds", IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, July-December 2013.

[117] Renjith P and Sabitha S, "Survey on Data Sharing and Re-Encryption in Cloud", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 2, no. 2, pp. 465-477 February 2013.

[118] Ashraf E. Al-Fagih, Fadi M. Al-Turjman, Waleed M. Alsalih and Hossam S. Hassanein, "A Priced Public Sensing Framework for Heterogeneous IoT Architectures", IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, pp. 133-147, September 2013.

[119] G. Ateniese, A.D. Santis, A.L. Ferrara and B. Masucci, ProvablySecure Time-Bound Hierarchical Key Assignment Schemes", Journal of Cryptology, vol. 25, no. 2, pp. 243-270, 2012.

[120] Heng He, Ruixuan Li, 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, October-December 2014.

[121] Noman Mohammed, Dima Alhadidi, Benjamin C.M. Fung and Mourad Debbabi, "Secure Two-Party Differentially Private Data Release for Vertically Partitioned Data", IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 1, pp. 59-71, January/February 2014.

[122] Ankatha Samuyelu Raja and Vasanthi A "Secured Multi-keyword Ranked Search over Encrypted Cloud Data ", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 10, October 2012.

[123] Yogachandran Rahulamathavan, Raphael C.W. Phan, Suresh Veluru, Kanapathippillai Cumanan and Muttukrishnan Rajarajan, "Privacy Preserving Multi-Class Support Vector Machine for Outsourcing the Data Classification in Cloud", IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 5, pp. 467-479, September/October 2014.

[124] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee and Wenjing Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615-1625, June 2014.

[125] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang, Yang Xiang, Mohammad Mehedi Hassan and Abdulhameed Alelaiwi, "Secure Distributed Deduplication Systems with Improved Reliability", IEEE Transactions on Computers, vol. 64, no. 12, pp. 3569-3579, December 2015.

[126]T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption", Springer Designs, Codes and Cryptography, vol. 77, no. 2-3, pp. 725771, 2015.

[127] Zhijie Wang, Dijiang Huang, Yan Zhu, Bing Li and Chun-Jen Chung, "Efficient Attribute-Based Comparable Data Access Control", IEEE Transactions on Computers, vol. 64, no. 12, pp. 3430-3443, December 2015.

[128] Jiani Guo and Laxmi Narayan Bhuyan, "Load Balancing in a ClusterBased Web Server for Multimedia

Applications”, IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 11, pp. 1321-1334, November 2006.

[129] Fu Yunhai, Ma Lin and Xu Yubin, “A Resource Scheduling Scheme for Spectrum Aggregation in Cognitive Radio Based Heterogeneous Networks”, Key Laboratory of Police Wireless Digital Communication, Ministry of Public Security, vol. 12, no. 9, pp. 100-111, September 2015.

[130] Suraiya Tarannum, Aravinda B, L Nalini, Venugopal K R, L M Patnaik, Routing Protocol for Lifetime Maximization of Wireless Sensor Networks, In IEEE Proceedings of 14th International Conference on Advanced Computing and Communications, IEEE Computer Society Press, Suratkal, India, ISBN: 1-4244-0716-8, pp. 401-406, 20-23rd December, 2006.

[131] Min-You Wu, “On Runtime Parallel Scheduling for Processor Load Balancing”, IEEE Transactions on Parallel and Distributed Systems, vol. 8, no. 2, pp. 173-186, February 1997.

[132] Wenhong Tian, Yong Zhao, Minxian Xu, Yuanliang Zhong and Xiashuang Sun, “A Toolkit for Modeling and Simulation of Real-Time Virtual Machine Allocation in a Cloud Data Center”, IEEE Transactions on Automation Science and Engineering, vol. 12, no. 1, pp. 153-161, January 2015.