International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 13237-13244

Security challenges of Big Data storage in Cloud environment: A Survey

S.Subbalakshmi[1], Dr. K.Madhavi[2]

[1]Research scholar, Department of CSE, JNTUCEA, Ananthapuramu, India.
[2]Associate Professor of CSE, JNTUCEA, Ananthapuramu, India.

Abstract

Big data is a collection of huge amount of large datasets and data volume but traditional management process cannot handle the big data storage.With the growing amount of data, the demand for big data storage increases. By placing the data in the cloud,that data is available to anyone from anywhere.Cloud computing is an emerging service-oriented framework for performing distributed and parallel computing over big data storage. Because of the increasing benefits of cloud computing in terms of cost, storage, and scalability and it is also focused by each data providers and institutions for out sourcing their data from the local servers to remote cloud servers, which has become a common trend. This raised major concerns about data security for cloud data storage and the enthusiasm in provisions of improvising the data consistency and privacy, which is causing the major hurdles towards the adoption of clouds services. In order to address this problem, this survey investigates the issues and challenges towards big data storage,data protection, privacy issues,and data accessing, controlling the shared data in the cloud.

Keywords: Data Protection, big data storage, data protection,Access Controlling.

INTRODUCTION

Big Data' is a term used for massive collection of data that is huge in size and growing exponentially with time. The data is being generated from several sources such as Social media, usage of Search engines, Sensors, Banking transactions, Financial applications etc.,and that data may be structured, unstructured or semi-structured.Big data is so large and complex that none of the traditional data management tools are able to store or process it efficiently.The 3 major characteristics of big data are:

Characteristics of Big Data	
Volume	Increasing data, storage space also increases, analysis /processing of data increases and time-consuming
Velocity	The speed of data retrieving, data storing is very quickly. Data flows continuously from source to destination like social media, companies, mobile devices
Variety	Structured (tables,numbers etc.), unstructured (videos,photos etc.), semi-structured (XML,.csv files etc.)

Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed to compute infrastructure capable of hosting end-customer applications and billed by consumption". Most of the users can upload the data in the cloud because they can access it from anywhere. Cloud computing is a promising technology that provides an attractive model to host and deliver services over the Internet.

The 3 major services offered by Cloud computing are:

a). Software as a service (SAAS): Based on subscription simply accessing the software via the internet instead of installing the software ex: Net flex, Google apps etc.

b). Platform as a service (PAAS): Platform allows tools to customers to develop, executing environment for programming languages, deploying, testing, updating. Ex:Force.com, Windows Azure, Heroku, AWS Elastic Beanstalk, Google App Engine.

c). Infrastructure as a service (IAAS): Infrastructure offers the users, can access the computing resources such as servers, storage and networking. Instead of purchasing the hardware devices, users can pay Iaas on demand, storage scalability on demand. Ex:Amazon Web Services (AWS), Linode, Cisco Metapod, Microsoft Azure, and Google Compute Engine (GCE).

The IAAS service offered by Cloud Computing is the best solution towards Big Data storage as the cloud resources are scalable in nature. The benefit of cloud storage isthat the user can access the data from anywhere. Subscribers can pay to the cloud storage provider (IAAS provider)for the amount of data transferring in and out of the cloud storage.Many organizations and individuals use cloud services to share information and collaborate with partners. However, the cloud provides an abstraction of the underlying physical infrastructure of the customer that caused the information security problem while storing the data in a virtualized environment without physical access. Even though the huge advantages of cloud computing paradigms are exciting for IT companies, researchers and potential cloud users, the security issues in cloud computing will become a serious obstacle, And if not properly addressed, it will impede the wide application and use of cloud computing in the future [1], [2],[3]. It is losingpopularity mainly because of its "Internet-based data storage" and "management" issues towards providing data security and privacy incloud computing [4], [5], and [6].

Cloud computing introduces a new system of service delivery to the IT development requirements and provides IT concept service. It has replaced IT functions capabilities in organizations and redefined all IT designs that affect "data performance", "reliability", "efficiency", and "security of data" networks [7], [8], [9]. However, service providers

should pay attention to data protection mechanisms as the characteristics of cloud deployment models differ from existing systems. With cloud infrastructure and platform providers (such as Amazon, Google, and Microsoft), most cloud app providers dedicated in providing cloud clients more flexibility and user-friendly data storage services. Client data outsourcing is a universal service that has become a clear trend in cloud computing.

Many different approaches have emerged to deal with various attack vectors within the information system. These methods include "firewalls", "intrusion detection systems", "intrusion prevention systems", "virus "scanning programs", "access control mechanisms", and "real-time monitoring". Each method emphasizes the specific range and type of potential attack vectors [10], [11]. In addition, the architecture, technology, and requirements of the management information system require stringent cyber defense methods. Specifically, ensuring the security of a single component defines a significantly different problem than a homogeneous cloud computing architecture. In particular, cloud computing architecture derives several unique attributes in its many forms. These include, but are not limited to, joint needs for multi-tenancy, dynamic lease, multiple operational domains, shared infrastructure, and policy definitions. These attributes need access control mechanisms that similarly promote these attributes.

Protecting information from cyber-attacks, malware, and internal cyber threats is a challenge. Attacks on "authentication" and "authorization" in access control are one of the potentially valuable attacks on distributed architectures. The security structure helpsto analyze a "trust management systems" to develop innovative authentication and authentication problem solutions through trusted management and privacy policies [8], [12], [13].On the other hand, cloud services are very dynamic, distributed and opaque, so establishing and managing trust between cloud service providers and consumers is an important challenge [14], [15]. This survey is designed to explore various degrees of acceptance of cloud data security related to data storage, privacy and access controlling management.

In order to have a trustful design, it is very important to have reliable service model or framework which can provide the required confidence in the data privacy to increase the usage of cloud service.The paper is organized as follows: In section 2, Model of Cloud Computing and its services are discussed, in section 3, Data Security and Privacy issues in cloud storage are discussed, in section 4, Protection and Security for Big Data in cloud are discussed, in section 5, Access Controlling for cloud data is discussed, in section 6, Related works are discussed, and in section 7, the survey has been concluded.

MODEL OF CLOUD COMPUTING AND ITS SERVICES

Cloud computing is a developing model that engages the enlargement of relevant technology to deliver widespread “computing power", "storage", "high availability" and "relatively low cost". Cloud service providers claim to provide better security, reliability, sustainability, cost-effectiveness, and support from the IT systems of the individual organizations. These features make it possible to transfer businesses from individual systems to the cloud and make it accessible via the Internet. The nature of "dynamic", "high scalability" and "extensive computing resources" make the cloud environment ideal for collaborative research and data exchange.

The "National Institute of Standards and Technology(NIST)" characterizes the cloud computing [16] as, "*Cloud computing is a model that can access shared configurable computing resource pools anytime, anywhere, and can be rapidly configured and published with minimal administrative effort or service provider interactions*". It provides applications and services with the abstraction of the underlying infrastructure and mechanisms. NIST designed a cloud model layer, as in Fig. 1.

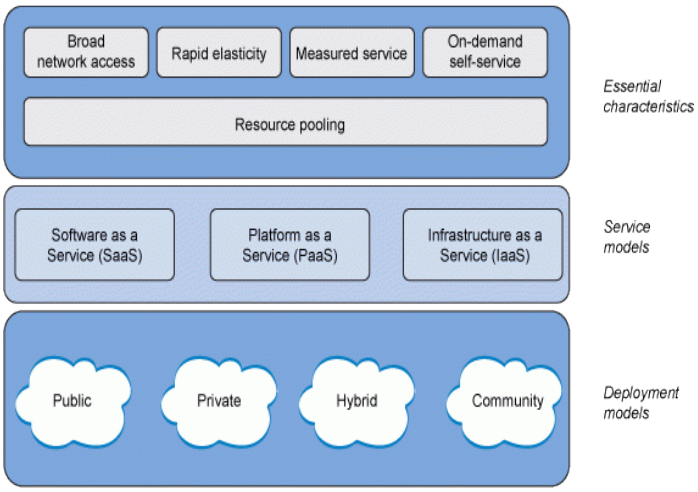

Figure 1. Designed Cloud ModelLayers by NIST [16]

A cloud model according to Fig.1 can be featured according to their functionality as, "Resource Pooling", "On-demand self-service", "Measuring service", "Rapid elasticity", and "Broad Network Access". Each of these has their characteristics to provide service according to the client requirements. It categorizes the services according to the kinds of service model it provides as, "Software as Service (SaaS)" and "Platform as Service (PaaS)", "Infrastructure as a Service (IaaS)" over dissimilar cloud organized models.

NIST categorizes four deployment models based on underlying infrastructure. The public cloud is a highly demanding design model because it offers the most significant and useful features of the cloud, such as "low costs", "extensive computing power", "rapid scalability", etc. However, while dealing with the public cloud number of concerns and risks arise in the migration of the real-time applications.

- **Public Cloud:** This type of cloud environment is provided to everyone through CSPs. Most consumers share a public cloud, which causes low consumer costs for personal consumers. However, consumers have little control over cloud infrastructure compared to private and

community clouds. Additionally, the data will be shared with anonymous individuals at a substantial level. This deliberation should be captured into consideration earlier than collecting responsive data in a public cloud.

- **Private Cloud:** Clouds that implement this deployment pattern are used by an organization. It is possessed and operated, or the third party is responsible for providing private cloud services. In general, private clouds provide high-superiority service. Nevertheless, it entails a considerable investment and administration attempt.
- **Hybrid Cloud:** Hybrid Clouds is a combination of many cloud infrastructure combined with some technology by facilitating interoperability among cloud services. Hybrid clouds include "private", "public" and "community cloud" infrastructure.
- **Community Cloud:** Some organizations may care and share similar needs. Deploying a shared cloud environment can make these companies profitable, supervised by one or more participating associations, or an intermediary party. The community cloud can become anexcellent alternative for medium-sized enterprises and partially manageable cloud services at a lower cost.

The existence of different cloud models for different services provides the needed reliability and security as per the type of data service opted by the data owner. But the open nature of cloud data storage raises a concern for data privacy and its security. Even though the cloud infrastructure is designed to provide low-cost storage and accessibility but it raises a big question over the risk of leakage of confidential data and its privacy. We discuss the major concern and security issue which are impacting the data storage and affecting cloud reliability.

DATA SECURITY AND PRIVACY ISSUES IN CLOUD STORAGE

Many incidents are reported in [8], [10], [11], [14], [17] on server down or fraudulence in recent times in the cloud service models causing the suspension of the cloud services. Significant cloud services data infringements have also come into sight from time to time [18], [19]. In addition, cloud service providers (CSPs) can perform volunteer reviews on the customer data for different inspirations. Therefore, it argues that the cloud is not naturally safe or reliable from the cloud's perspective. Cloud clients have difficulties in expecting cloud servers without strong security, privacy and reliability.

Although cloud computing is growing rapidly and is being used by the growing number of organizations worldwide, confidentiality and data integrity issues are not being adequately addressed at present. Storing sensitive data in the cloud, with no knowledge of where the data are actually accessed and accessed via the internet, enhance the threat of compromising data. The menace of leakage of classified data and privacy violations in the cloud significantly hampers the widespread adoption of this technology[20], [21], [22].

Cloud Data Security

CSPs provide different steps to protect data stored in the cloud. Most CSPs offer encryption capabilities to consumers, so all data is transferred and stored in the encrypted form on the cloud storage system [32]. However, important management challenges and internal threats should be noted. Certification of CSP guarantees some level of customers. However, consumers have no guarantee of complete self-examination of cloud information, such as guarantee of unrestricted resources or "30-dayopentryout". In the period of the registration procedure, customers are often asked to provide additional information that is required for providing personalization of the service. The most frequently asked information of the user is partially compelled with more information than is necessary for the use of the service. This information can beutilizedby the malicious objects for fraudulent purposes.

Cloud Data Privacy

Cryptography means a set of techniques and algorithms to protect data. Cryptography converts plaintext into ciphertext by using many algorithms. There are various algorithms i.e. public key cryptography, attribute-based encryption etc. By using these algorithms data encrypted, that encrypted data stored into cloud, still there may be leakage of information. Traditional encryption schemes do not provide efficient privacy to cloud. Each person stores specific information onto cloud. Privacy is a major security concern. The privacy in cloud consist of major factors: anonymity, data access from cloud, data stored into cloud etc. There are different privacy preservation methods: data anonymization, notice and consent and differential privacy etc.

Cloud Data Reliability

Reliability is most important in cloud storage. Users store the encrypted data into the cloud. Only authorized persons can update and access that data. Unauthorized users can access the encrypted data, but they cannot decrypt the data.A good storage agreement between users and cloud needs to support concurrent modification by multiple users. However, the reliable protocol supports the limited types of operation. Most of the manipulations can be done by the authenticated client.

Cloud Data Storage Threats

Customers can view remotely stored storage systems as the same system in which they are using. The use of a unified interface presentation can moreover be utilized by consumers to hide the complexity of underlying communications. This is a very important concept and cloud computing moreover shares it. Cloud users can view the cloud as a "single" system, but this view prohibits the complete risk model to set up data in the cloud. But it only provides the users with the flow of data in and out of the Cloud. So accordingly the types of vulnerability to the storage data are capable of being classified into the following types of intruders:

- **Natural:** The "errors" can be triggered by both internal and external infrastructure, but other errors may naturally result from software or hardware failure. For instance, as "Google pushes the software updates to Google Docs" [23]. The software breakdown transformed the distribution configurations of many consumers, including individuals with troubleshooting users who shared records in the past.
- **Insiders:** Most serious threats arise from existing or former workers of the CSP. Workers might have a complex understanding of real mechanism, which adds the security, and might include straight access to the data directly or through other methods as part of their transaction. Their insight may be out of curiosity or misuse as it involves.
- **Outsiders:** These intruders try to ignore/disassemble the outside of the system's security infrastructure, or impersonate as a genuine examination to target consumers. Their inspiration arises from straight forward in quisitiveness or misuse.

Even though data storage can be effectively managed through addressing different types of attacks or malfunctions affecting the data storage issue, but data owners still have the worry towards its accessibility and protection from the anomalous users to maintain the data privacy [33], [34]. To have a secure control over the accessibility, it is important to have effective data protection and security methods to control the data confidentiality, integrity and increase the data owner reliability over the cloud storage and accessibility. In the next section, we discuss the process of data protection and the methodology to control from the inaccessibility by the unauthorized users.

PROTECTION AND SECURITY FOR BIG DATA IN CLOUD

With the growth of data, bigdata storage also increases. So users can place the data in the cloud. Users can download and upload data from anywhere. Security and protection issues come whenever uploading downloading data into the cloud. Data protection from the intruders and controlling user accessibility in the CSPs are two major and foremost requirement which most likely effects [24]. Therefore, security and privacy requirements between the users and the CSPs are correlated. It also has to address four classic security constraints related to "Confidentiality", "Integrity", "Availability", and "Authentication". Protecting data is an important necessity when designing the IT infrastructure of the organization [1], [2]. These requirements are more difficult when data is moved to the cloud, and data can be accessed via the Internet. Therefore, assigning such systems must have strong authentication and access control mechanisms. Information handled in the cloud may be sensitive and therefore are subject to several confidentiality measures. Based on relevant literature and our analysis, we describe the general security and privacy requirements for the data located in the cloud.

Data confidentiality is the primary security factor for data protection. Providing these services in cloud computing is very important since the distinctive of cloud computing is due to the increased hazard of data breaches such as "remote data storage", "lack of network boundaries" and "third-party cloud service providers", "multi-tenancy" and "large-scale infrastructure sharing".[4], [5], [6]. The simplest way to ensure data confidentiality is to encrypt all susceptible data while "stored", "processed", and "transmitted" to the cloud server.

Data encryption offers an effective way to protect data confidentiality [21]. The cost reduces effectiveness and elasticity of data handling. Another methodology to address "data confidentiality" is to eradicate responsive data and to store as non-critical data in the cloud. This greatly simplifies the complexity of managing systems because key distribution and management are no longer needed. The main disadvantage of this solution is that information is lost by removing important information. In many application situations, this process preserves data confidentiality but makes the data useless.

In cloud computing, different variety of data in various applications can have unique characteristics in expressions of "dynamic characteristics", "data processing operations", and "sensitivity". It is non-realistic to provide a consistent explanation to protect data in every one of these applications. As an alternative, it can choose how it wants to protect user data based on the nature of the user data. To do this, it must first sort the data according to a predefined nature. For example, if the cloud has relatively static data, such as the system's log data and it might be necessary to encrypt the data to permits for effortless data inquiry and retrieval procedures.

Data integrity in cloud computing is another major security issue. This security guarantee is required for communication between cloud users and cloud servers, as well as information from a cloud server. In particular, cloud consumers can take care of data integrity when outsourcing critical data assets stored in the cloud. The unlimited elasticity of resources provided by cloud computing enhances the ability to store and to process cloud user data. The cloud users (data owners) replicate high-quality data services to geographically dispersed cloud servers and agree to customers to provide efficiently accessibility of data through local cloud servers.

ACCESS CONTROLLING FOR CLOUD DATA

Access control (AC) is a significant element of every information system[5], [6], [19], [25]. It can be defined as, "*Access control is the process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied"*. Access control rules are imposed by the rules of access control by means of authorization. Due to the wide number of use cases, an inherently difficult task is to indicate all access control requirements. The following describes the requirements for secure security mechanisms: the cloud considers general safety requirements for secure data collection and collaboration.

- **Co-operation of AC:** The various legal and moral policies of participating organizations face challenges for cloud access control. Data may be requested or rejected by the law of the country in which the country is living. In some countries, moral approval may be required to fulfill the request. The access control system supports such restrictions and situations and provides additional information about requests for the request to modify the request and to provide proper access to the negotiations. In addition, the access control system is able to automatically access or communicate.
- **Filtered-Level AC:** To support various customers' participation, the cloud access control system must support extensive range resource types. Basic operations must be supported to read, write, execute, and delete. Additionally, micro-container access methods can be supported in accordance with the specific requirements of management operations. In some cases, since an operation intention is strictly required, so the control system must sustain in the feature.
- **Distributed AC:** Collaboration in the cloud can be done in association with various participants of various infrastructures and the centralized access control system does not meet with the requirements of this ecosystem. Existing systems relate most "role-based access control", which is appropriate for uniform environments, where the variety of the data, characters, and functions are allowed. However, the system must consider support for more diverse materials, users,and rules, which are assigned to clouds and spread across many countries.

Systems for Data Access Control in Cloud

The requirements for cloud access control differ from the case to the case, as the Cloud environment needs to provide services to different customers. The number of access control models and systems for Cloud has been developed to address some required sets [5], [6].

- **ABE-FG - "Attribute-Based Encryption Fine-Grained Access Control":** Li *et al.*recommended a good grade access control in the cloud based on character-based encryption in their work [25], [26]. This access control mechanism provides better liability and user cancellation. There are two types of ABE in this model. The first one is the key policy ABE (KP-ABE), which has been implemented for a private key, which is allocated to the user. Files that match the policy can decrypt this key with the embedded policy. The latter is based on the cipher text policy ABE (CP-ABE) where access policy is accessed to cipher text with every file. The consumer key has dissimilar properties, describing the structure of the entry. If the attributes go with the file structure the user can access the file. This system includes "data owners", "consumers", "cloud providers" and "third-party auditors". A "Broadcast encryption" is used by the data owner to define consumer groups to access client files. The user can access the file if the number of attribute values matches the policy, at least the same as the predefined limit value.
- **FG-D - "Fine-Grained Data Access Control":** Wang*et al.*propose Hybrid Access Control Model [19], [25] using "attribute-based encryption (ABE)", "proxy re-encryption" and "tap encryption". Files have features and public key in accordance with these features. Logical expressions define access to files structure on public key properties. Data file collections are described for every client. Files are encrypted by "symmetric keys". The Symmetric keys are encrypted with ABE, depending on the key policy. To retrieve the user, the data owner specifies the minimum properties and modifies the public keys according to specific features. Then, they produce "proxy re-encryption keys". Data owners send "consumer ID", "attribute set", "proxy re-encryption keys" and "public keys" to the cloud server. The cloud server will retrieve the specified user and store the updated keys in the Properties list.
- **H-ABE - "Hierarchical Attribute-Based Encryption Access Control":**S. Wang*et al.* [26] have mentioned encryption based on a range of attributes[26]. Access control system is through merging "hierarchical individuality - based encryption (HI-BE)" and "cipher text policy based attribute encryption (CP-ABE)".The excellence includes "root master (RM)" and "domain masters (DM)". RM is responsible for the production and distribution of keys. DM is responsible for providing the essential features and delivering keys and distribution of keys to users. Each user has an ID and some features. The user's location is determined by the ID and the public key of the user's administration.
- **RB - "Role-BasedAccess Control ":**Z. Yan*et al.*mentioned RB-AC [27] to the cloud. The work is administered in two steps according to the control of the entrance. The first user is certified based on the provided features. Then, user characters are acknowledged and the consequent access rights are allocated to the consumer. If users are already registered in the database, authentication is done through the identity assessment features. Otherwise, authentication can be achieved by the validation credentials provided by the user. Likewise, recognition is assigned to the characters based on the identification.
- **TRB - "Task-Role Based Access Control":**K. Yang *et al.*proposed TRBAC [28] which distinguishes the characters from functionality, as opposed to RB-AC, the characters and functions are combined and classified based on active and inactive access control. Additionally, tasks should not be inherited or inherited. Active access control is required for functions that are part of the workflow. In contrast, actions that are not a portion of the execution necessitateactive access control. The TRB-AC consumers are allocating to the roles, the roles allocated to the task, and the functions assigned to the permissions.

RELATED WORKS

Cloud computing has revolutionized the IT concept into service [4], [7], [8], [9], [17], [29] with establishing an innovative computer service deliverance model for the IT development requirement. It has improved IT performance capabilities in society and has rebuilt each IT constructions affecting the "performance", "reliability", "efficiency", and "security" of the cloud data system. However, as the features of Cloud Assignment models differ extensively commencing the existing utilization of the service provider, which must be more concerned about the data protection systems.

Security is one of the major challenges facing the cloud environment. The 88% of cloud consumers request access to their data and request greater consideration to reverses, such as possible cloud consumers [5], [6], [25], [30] physical location, data management and security administration of their cloud data in virtual environments. This indicates that users recognize clearness and security over cloud information. The service provider may be fully controlled by managing the cloud service of a cloud service, but some cloud service providers do not allow the user to use cloud information in the cloud.

Wei Li *et. al*. [6] presents "Attribute-Based Encryption (ABE)" is considered a capable cryptographic management tool that ensures direct control of the data owner on data in public cloud storage. The former ABE projects have the sole power of managing the entire property set, which brings one-point barriers in both security and performance. It runs a multi-proprietary CP-AE access control plan for public cloud storage named TMACS, in which many executives jointly manage the uniform properties. The new limit-multi-authoritarian TMACS suggests the effective implementation of the traditional multi-authoritative project with TMACS. This creates a hybrid project that is appropriate in the authentic situation, in which the characteristic sets consist of different characteristics and features from multiple authorities jointly perform the entire property subdivision. It does not explain the reasons for selecting the master key for the target value for hidden sharing, feature set, and targeted communication design protocols.

V. Chang *et. al* [8] proposed a CCAF multi-layer security protects real-time data, and it has three layers of security: 1) "firewall and access control"; 2) "Identification Management and Intervention Prevention", and 3) "Conversion Encryption". It has taken two sets of ethical-hacking experiments in intrigue testing. The CCAF multi-layer security protects data from speedy data expansion because of security violates. This method provides real-time protection for all the data, prevents more threats and removes the systematic system in the data centre and provides a comprehensive explanation of cloud security supported by a comprehensible structure that affects the performance of user-accessed service, business process modelling. It can be further evaluated in real-time scenarios to measure efficiency.

M. Anisetti*et. al*[7] provides a tough and cohesive guarantee strategy based on authentication, which completely resolves cloud requirements. The Authentication Scheme provides a solution to the management of the certificate lifecycle, which is an automated and increasing method for certification transforming the cloud multi-layer and dynamics nature. Each piece of cloud behaves as expected and increases the confidence of cloud consumers according to their requirements. This defines an automated approach to stability scrutiny between requirements and models, based on the chain's trust supported by the certification scheme. The project does not consider service combinations based on affiliate service certification and cost-efficient certification to enable a certification-based combination that supports cost optimization on the side of Cloud Providers.

S. Lins*et. al*[14] continuously explores dynamic certification requirements to ensure secure and reliable cloud services and installs reliable cloud service certifications. Cloud service systems and processes are widely adopted, and functional certification of cloud services is technically and economically viable. Most consumers demand transparent, reliable certified cloud services, and the provider can start opening up for dynamic certifications.

Chi Chen *et. al*[20] proposes a search mechanism in the ciphertext cloud storage. It explores the difficulty of preserving a semantic association among various simple documents in relation to the encrypted documents and provides a method to improve the performance of the semantic search. The proposed method has an advantage over the conventional method of ranking privacy and the relevance of the retrieved records, as it analyzes search competence and security beneath two admired threat patterns. The work is focused only on data privacy but the effectiveness and accessibility of various search users are not discussed.

S. Wang *et. al*[26] presents has redesigned the attribute-based data sharing program in cloud computing. Advanced key protocol resolves major escrow problems. It introduces the concept of expression, provided to enhance the attribute expression, which not only expands expression from the binary but also reduces the complexity of access policy. KA and CSP managers and malicious system outsiders increase data privacy and confidentiality in the cloud system against semi-reliability of the KA and CSP. In addition, improvement of attribute expression is an added characteristic, which can not only describe the state characteristics of the arbitrary but reduces the complexity of the admission policy. Data privacy and privacy are assured in the proposal but data owners and data request cannot be assessed by the trust. This can be done to evaluate trust management models for better cloud security.

Zhongma Zhu *et. al*[31] designed a safe anti-strategic data sharing plan for cloud dynamic groups. In this project, users can securely obtain their private keys from "Group Administrator Certification Authorities" and "Secure Communications Channels". This project is capable of effectively supporting dynamic groups when new users are added to the group or withdrawn from the user and other users' private keys do not need to be reconnected and updated. Users can cancel even if they are not trusted. User confidence assessment is not considered before withdrawal in the group.

Joseph K. Liu *et. al*[24] provided a "two-digit data protection" document for a cloud protection system, which allows the sender of the data to hide the recipient's information, but the

recipient is his privacy key and security to get customer information. The solution increases the privacy of the information and provides a device recovery, so that if the device is withdrawn, the equivalent ciphertext will not be mechanically detected by any data owner from the cloud server. The work focuses largely on the confidentiality of data and device control, but it does not evaluate trusted users and misrepresents the user reviews.

Zheng Yan *et. al*[27] focuses on storing encrypted data with encryption running for "secure", "reliable", and "green cloud storage service", particularly for large data systems.It suggests function based on the encryption name ABE, to copy the encrypted data stored in the cloud as it supports the ability to access data at the same time. Existing solutions to copying are subject to brute attacks and do not support data access control and returns smoothly. It is based project to support encrypted data stored in the cloud at the equivalent time supports protected data access control. This proposal does not evaluate competitive data ownership verification and flexible compensation for supporting copy and data access controlled for schema optimization.

CONCLUSION

Data privacy and security are the main concerns of cloud computing. Big data is a collection of large volumes of data that cannot be handled by traditional architecture. To overcome this, the Cloud Computing architecture is being used by many organizations to store such volumes of data. However the major concern is regarding data privacy, security and access controls. In this paper, issues related to data storage security and access control are studied. Most of the research carried out on data security, privacy access cloud in cloud environment. The current approaches not work well with big data. To handle huge amount of data at any instance, it increases issues related to transfer of data, storage maintenance and access issues. Hence there is lot of scope for research in improving data security, privacy and access control.

REFERENCES

[1] M. Qiu, K. Gai, B. Thuraisingham, L. Taob, H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in the financial industry", ELSEVIER Future Generation Computer Systems, Vol. 80, pp. 421-429, 2018.

[2] Mitchell G. Goldenberg, Teodor P. Grant charov, "Enhancing Clinical Performance and Improving Patient Safety Using Digital Health", In Springer Digital Health. Health Informatics, pp 235-248, 2018.

[3] Y. Wang, B. Rawal, Q. Duan, "Securing Big Data In the Cloud with Integrated AuditIng", IEEE International Conference on Smart Cloud (SmartCloud) Pgs. 126 - 131, 2017.

[4] M. Dieye, M. F. Zhani, H. Elbiaze, "On achieving high data availability In heterogeneous cloud storage systems", IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Pgs. 326 - 334, 2017.

[5] Z. Liu, Z. L. Jiang, X. Wang, S. M. Yiu, C. Zhang, X. Zhao, "Dynamic Attribute-Based Access Control In Cloud Storage Systems", IEEE Trustcom/BigDataSE/ISPA, Pgs. 129 - 137, 2016.

[6] W. Li, K. Xue, Y. Xue, J. Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System In Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2016.

[7] M. Anisetti, C. Ardagna E. Damiani, F. Gaudenzi, "A semi-automatic and trustworthy scheme for continuous cloud service certification" IEEE Transactions On Services Computing, 2016.

[8] V. Chang, M. Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, 2015.

[9] B. Dong, R. Liu, Hui Wang, "Trust-but-Verify: Verifying Result Correctness of Outsourced Frequent Itemset Mining In Data-mining-as-a-service Paradigm", IEEE Transactions on Services Computing, 2015.

[10] N. A. Kofahi, A. R. Al-Rabad, "Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey", Advances in Networks, 6(1): 1-13, 2018.

[11] I. Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – Threats and Challenges", Journal of Computer Management Studies, vol. 1, no. 1, 2017.

[12] P. Johri, A. Kumar, S. Das, S. Arora, "Security framework using Hadoop for big data", International Conference on Computing, Communication and Automation (ICCCA) Pgs. 268 - 272, 2017.

[13] W. Tang, K. Zhang, J. Ren, Y. Zhang, X. Shen, "Lightweight and Privacy-Preserving Fog-Assisted Information Sharing Scheme for Health Big Data", IEEE Global Communications Conference (GLOBECOM 2017) Pgs. 1 - 6, 2017.

[14] S. LIns, P. Grochol, S. Schneider, and A. Sunyaev, "Dynamic Certification of Cloud Services: Trust, but Verify", IEEE Computer and Reliability Societies, 1540-7993/16, 2016.

[15] F. Corradini, F. Angelis, F. Ippoliti and F. Marcantoni, "A Survey of Trust Management Models for Cloud Computing", In 5th International Conference on Cloud Computing and Services Science, Pgs. 158-162, 2015.

[16] P. Mell, T.Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.

[17] T. Noor, Q. Sheng, L. Yao, S. Dustdar and A. Ngu. "CloudArmor: Supporting Reputation-based Trust Management for Cloud Services", IEEE transactions on parallel and distributed systems, Vol. 27, no. 2, Pgs. 367-380, 2015.

[18] C. Yanli, S. Lingling,and Y. Geng, "Attribute-Based Access Control for Multi-Authority Systems with Constant Size Ciphertext in Cloud Computing Computing", IEEE, China Communications, Vol. 13, Pg. 146 - 162, DOI- 10.1109/CC.2016.7405733, 2016.

[19] M. Xiao, M. Wang, X. Liu, and J. Sun, "Efficient distributed access control for big data in clouds", Proc. - IEEE INFOCOM, vol. 20, no. BigSecurity, pp. 202–207, 2015.

[20] C. Chen, X. Zhu, P. Shen, J. Hu, S. Guo, Z. Tari, A. Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 4, 2016.

[21] K. Liang, W. Susilo, and Joseph K. Liu, "Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, 2015.

[22] S. Wang, J. Zhou, Joseph K. Liu, Jianping Yu, J. Chen, WeixinXie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, Volume:11, Issue: 6, 2016.

[23] J. E. Vascellaro, "Google Discloses Privacy Glitch. English. Wall Street Journal", LInk: http://blogs.wsj.com/digits/2009/03/08/1214/, 2009.

[24] J. K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System", IEEE Transactions on Computers, 2015.

[25] T. Yang, P. Shen, X. Tian, C. Chen, "A Fine-Grained Access Control Scheme for Big Data Based on Classification Attributes", IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) Pgs. 238 - 245, 2017.

[26] S. Wang, K. Liang, Joseph K. Liu, J. Chen, JianpIng Yu, W. Xie, "Attribute-Based Data Sharing Scheme Revisited In Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 11, 2016.

[27] Z. Yan, M. Wang, and Yuxiang Li and A. V. Vasilakos, "Encrypted Data Management with Deduplication In Cloud Computing" IEEE Cloud Computing Computer Society, 2325-6095/16, 2016.

[28] K. Yang, X. Jia and K. Ren, "Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 12, December 2015.

[29] A. Bonguet and M. Bellaiche, "A survey of Denial-of-Service and Distributed Denial of Service attacks and defenses in cloud computing", Future Internet, vol. 9, no. 3, 2017.

[30] T. Pasquier, J.Singh, J. Powles, D. Eyers, M. Seltzer, J. Bacon, "Data provenance to audit compliance with the privacy policy in the Internet of Things Personal and Ubiquitous Computing", Vol. 22, pp 333–344, 2018.

[31] Z. 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, 2016.

[32] R. Chen, Yi Mu, G. Yang, FuchunGuo and X. Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage IEEE Transactions On Information Forensics Security,1556-6013, 2015.

[33] S. Aldossary, W. Allen, "Data Security, Privacy, Availability,and Integrity in Cloud Computing: Issues and Current Solutions", Int. J. Adv. Comput. Sci. Appl. , vol. 7, no. 4, pp. 485–498, 2016.

[34] G. Aswini, R. Mervin, "A Survey on Cloud Security Issues and Techniques", International Journal of Computer Science and Application, vol. 4, no. 1, pp. 125–132, 2016.