IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

Data Access Control Techniques and Security Challenges in Cloud Computing: A Survey

S.S. Manikandasaran[1*], S. Sudha[2]

[1*]Department of Computer Applications, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India
[2]Department of Computer Science, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India
**Corresponding Author: arthikumari10@gmail.com, Tel : +91 9095343145*

Available online at: www.ijcseonline.org

Abstract— Cloud computing is a distinctively different environment, that has captured many hearts and it has emerged as a powerful computing environment with the provision of high standard data storage mechanism and sharing the data efficiently among multiple users across the globe. As it is dynamic in nature, it offers innumerable advantages such as flexibility, resource pooling, elasticity, and scalability, etc. One of the important features of cloud computing is the multitenant environment, which enables outsourcing data into the server; however many security challenges incorporated with this are unauthorized access, data privacy, malicious attacks, and threats. Accessing the data from the server plays a very important role in cloud computing environment. This paper analysis several data access control schemes have been described to ensure the data access as convenient and efficient as possible. Access control is a security technique that defines the access policy, and it can be used to legalize who or what can use various resources in a computing environment. It is necessary to have tightly controlled system to access the data securely and the data access risk must be addressed. This survey explores myriad ways of Cloud Data Access Control Techniques and its challenges.

Keywords— Cloud Computing; Access Control System; Security Technique; Authentication

I. INTRODUCTION

IT is currently in the midst of a once-every-20-years tectonic shift, according to Mohindroo, Vice-President of Oracle Cloud. The most recent 1990s shift from client/server computing to the internet, is now being supplanted by the transition to cloud computing. The upheaval is far-reaching and impossible to avoid. Cloud Computing systems and services should provide authorized, granular, auditable and appropriate user access, and ensure the appropriate preservation of data confidentiality, integrity, and availability in accordance with the Information Security Policy. Access control systems are in place to protect the interests of all authorized users and IT systems must provide a safe, secure and accessible environment to work. As per the NIST (National Institute of Standard Technology) definition Cloud Computing has been described as "a model of ubiquitous, flexible, more convenient and on-demand network access for computing resources such as networks, servers, storage, applications and services with less effort or minimal service provider's interference [1]. Cloud-based data storage and accessing data are very complicated tasks in cloud computing environment.

A. Cloud Computing Models

Cloud Computing offers various services and models, which make the cloud environment feasible and accessible to end users. The two important working models of cloud computing are Deployment Models and Service Models [2].

- Deployment Models: Deployment models define the type of access to the cloud. There are four types of Cloud models such as Public, Private, Hybrid, and Community.

- Public Cloud: In this model, systems and services are easily accessible to the public. Due to its openness, it is less secure. Windows Azure, Google App Engine (GAE), Amazon web services (AWS), IBM's Blue Cloud, and Salesforce.com's (Force.com) are an example of this model.

- Private Cloud: The Private Cloud allows an organization to access the systems and its resources. It is considered as more secure since it is private in nature compared to the other models.

- Community Cloud: The Community Cloud allows systems and services to be accessible by a group of organizations. E.g. Universities.

- Hybrid Cloud: The Hybrid Cloud combines the features of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using the public cloud.

B. Service Models

- Anything-as-a-Service (XaaS): is a kind of service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

• The Infrastructure-as-a-Service (IaaS): Third party cloud service providers such as Amazon Web Services, Microsoft Azure or Google provide virtualized computing resources over the Internet. It also provides high-level Application Programming Interface (APIs) and the user can access the resource based on their demand. As it provides various computing resources, the user can deploy and run any kind of software which may include operating systems and various applications.

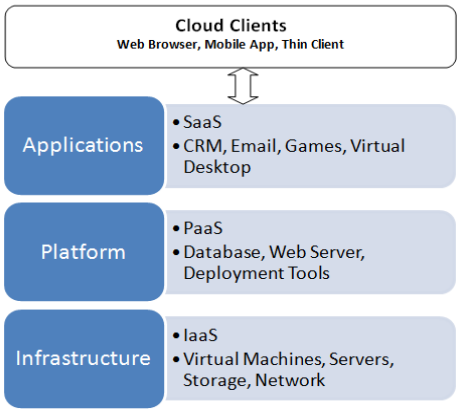

Fig. 1 Service Models of Cloud computing

• Platform-As-A-Service (Paas): Platform as a Service (PaaS) allows organizations to build, run and manage any kind of applications without the support of IT infrastructure. It is also called as application platform-as-a-service (PaaS). Paas offers two different kinds of services, (i) as a public cloud service provider where a user is able to deploy software with less configuration, and also the provider provides various services such as networks, storage, OS (Operating System), database and other services to the user to deploy their applications. (ii) As a private cloud service inside the firewall. It can reduce your management overhead and lower your costs. PaaS also makes it easier for you to innovate and scale your services on demand. It provides pay-as-you-go platform to the developers hence they can build and deploy any kind of applications.

• Software-As-A-Service (SaaS): It is referred as "On-demand Software". The user can access any kinds of software using a thin client with the help of web browser. Software as a service (SaaS) replaces the traditional on-demand software with software that is licensed on a subscription basis. It is centrally hosted in the cloud. A good example is Salesforce.com. Without any downloads or installation, most of the SaaS applications are can be accessed openly from server. However, some SaaS applications require plugins.

II. Related Work

In Cloud Computing Environment, different access control technologies are available to support the different access control models. Many researchers have presented various Data Access Control Technologies which allow the user and the needy to access the data efficiently, which are as follows.

M. Kallahalla et al. [3] proposed solutions for protecting data in a Cloud environment based on traditional Encryption schemes such as a Symmetric key or Asymmetric key (Public Key) cryptography. Based on trust management, controlling access to the stored data at CSP was performed. It worked well, but it has disadvantages that the key management is difficult and the access control is not flexible enough.

Huaqing Lin et al. [4] proposed cloud data access control system called CDController through reputation evaluation and they introduced a Reputation Center (RC) to help data owners control the access to their personal data based on integrating trust management and reputation during cloud service fulfillment. CDController exhibits secure control of the access to the data stored at CSP data center according to the reputations of cloud computing entities by applying Proxy Re-Encryption (PRE) in the absence of data owner or it has no idea how to control the data access. The disadvantage of this scheme is that the data owner should be online to issue PRE keys to CSP.

Chase et al. [5] implemented a scheme called "Multi-Authority Attribute-Based Encryption System", in which each authority would administer various domains of attributes. The important goal of this scheme is creating multi-authority ABE to avoid collusion attacks between users that obtain key components from different authorities. This system used the Threshold ABE schemes as its fundamental ABE system at each power; the problem of this multi-authority ABE scheme is in general orthogonal to finding more expressive ABE systems.

John Bethencourt et al. [6] implemented a highly promising scheme called Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This implementation explains that encrypted data can be kept confidential even if the storage system is less secure. It is more secure against the collision attacks. However, there exist two open problems of this scheme is that it may limit its wide deployment in commercial applications. One point is that when access policy size increases it causes expensive pairing cost during decryption. The other point is that one is permitted access privilege for unlimited times as long as his/her attribute set satisfies the access policy of a provided ciphertext. Though it is considered a strong one it may be undesirable in real-world applications (e.g., pay-as-you-use).

Xuejiao Liu et al. [7] proposed new data access control system named a Hierarchical Attribute-Based access control scheme. In this scheme, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is combined with a Hierarchical

structure of Multi-authorities using Attribute-Based Signature (ABS). Due to its Hierarchical structure, the scalability is improved and also it inherits Fine-Grained Access Control with authentication in supporting write privilege on outsourced data in Cloud computing environment. This scheme not only provides Fine-Grained Access Control but also authenticates users who store information in the cloud. In this scheme, the authorization scheme is developed upon XACML (Extensible Access Control Markup Language framework to enable effective data sharing in a secure and controlled manner.

Jin Li et al. [8] implemented a data access control system called "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing" where scalable and fine-grained access control systems are implemented based on Attribute-Based Encryption (ABE). This paper addresses the issue that the access policy is designed based on data attributes and the user accountability is implemented based on traitor tracing. This system is highly efficient and probably more secure.

The attribute-based encryption (ABE), was coined by Sahai and Waters et al. [9], has attracted much attention in the research community to design flexible and scalable data access control systems. For the first of its kind, ABE enables public key (Asymmetric Encryption) based one-to-many encryption. Therefore, it is considered as highly promising public key encryption techniques for realizing scalable and fine-grained access control systems, where different yet flexible access policies can be assigned to individual users.

Ruj et al. [10] proposed Distributed access control in clouds (DACC); it is based on a Multi-authority attribute-based encryption scheme that uses LSSS matrix to achieve an efficient encryption, decryption process. This model proposes a user with limited computational power requirements to the minimal overhead of the decryption process.

To access secured data in a Cloud Computing environment user required a flexible, efficient and scalable access control system. Zheng Yan, et al. [11] proposed an access control system called "Flexible Data Access Control based on Trust and Reputation in Cloud Computing", according to this system Attribute-Based Encryption and Proxy Re-Encryption schemes are used to have a data access control system based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers. To support diverse control systems and strategies, this system integrated the concept of Context-aware trust and reputation in a cryptographic system.

In cloud computing environment RBAC (Role-Based Encryption) provides flexibility on access control management. Zhou et al. [12] proposed a secure RBAC-based cloud storage system where the access control policies are put into effect by Role-Based Encryption (RBE). This scheme insists on RBAC policies on encrypted data stored in the cloud with an efficient user revocation mechanism so that RBAC policy specified user is able to decrypt the data.

Imad El Ghoubach et al. [13] proposed a system called "Efficient Secure and Privacy-Preserving Data Access Control scheme for Multi-Authority Personal Health Record Systems in Cloud Computing", where a multi-authority scheme with semi-outsourced decryption (MABE-SOD), and this system included proxy decryption server for carrying out decryption process. This scheme provided efficient attribute revocation scheme by outsourcing the ciphertext update to the server.

Mustapha Ben Saidi et al. [14] proposed a new model for specifying security policy on cloud data is "Trust Organization Based Access Control" (TOrBAC) which relies on the use of a recursive formula for calculating a confidence index. As it concentrates on trust management so much focus is required for security policy.

Dongwan Shin et al. [15] proposed a system called a policy-based decentralized authorization tool in cloud computing. Where access control architecture is designed based on XML-based security architecture and RBAC model. However, the model and tool do not support privacy preserving of the resources shared to users.

Somchart Fugkeaw et al. [16] implemented a scheme named "CLOUD-CAT: A Collaborative Access Control Tool for Data Outsourced in Cloud Computing." This paper proposed the concept that the resource (data) can be shared among multiple users. The administrative tool CLOUD-CAT enables flexible, secure and efficient multiple accesses control. It combines the features of Ciphertext Policy-Attribute-based Encryption (CP-ABE) and Role-based Access Control Model (RBAC) access control model. This tool provides a secure communication channel for multiple users to access the resource in Cloud Computing Environment.

Md Sadek Ferdous et al. [17] introduced the new scheme called "Decentralized Runtime Monitoring for Access Control Systems in Cloud Federations". This scheme proposed a runtime monitoring architecture for distributed access control systems: Decentralized Runtime Access Monitoring System (DRAMS). This model employs a novel approach called Block chain that supports data integrity and distribution and Access Control policy.

The proliferation of cloud computing bounce many challenges, one of the important challenges is data security. It is highly important to safeguard the user's data. To ensure data security in Cloud computing Jun Hu et al. [18], implemented a scheme called "Data Security Access Control Model of Cloud Computing." This paper deals an access control model for accessing the data securely based on MAC

Access Control. This paper proposes an access control model for accessing the data securely, analyzing the risk factor of data security. This model proposes three-stage access control technology strategies and management strategies which ensures data access security with high reliability.

Wenqing Tian et al. [19] introduced a new system called "Secure and Flexible Data Sharing via Ciphertext Retrieval for Cloud Computing". To achieve flexible sharing environment with minimal computation cost this system combined homomorphic encryption with TF-IDF weight vector model to implement a ciphertext retrieval scheme. The advantage of this scheme is computation cost is very minimal.

Attribute-based encryption (ABE) has emerged as a feasible solution to regulate the access control to the diverse set of users in cloud computing systems. Fawad Khan et al. [20] defined a scheme called "Owner Specified Excessive Access Control for Attribute-Based Encryption", Where Owner plays an important role in specifying the access policy for a specific attribution off data to be accessed. To avoid the repetition of the attribute, this scheme introduced a technique called LSSS (Linear Secret Sharing Scheme) that access matrix which leads to less computation in the encryption process the ciphertext size. This method provides data owner more privilege and this system can specify the access restriction to the user based on attributes.

The cloud environment is dynamic in nature and supports remote access for computation, storage etc. This environment demands Attribute-Based Encryption- access control models which provides the user to access the data stored in the cloud. RajaniKanth et al. [21] described an access control mechanism called "A dynamic attribute-based risk aware access control model (DA-RAAC) for cloud computing", it combines the features of KP-ABE (Key Policy-Attribute Based Encryption) and CP-ABE (Ciphertext-Policy Attribute-based Encryption). This model processes risk computation with attributes used for access control. This model proposes a new mechanism called risk engine which calculates the risk for granting/denying permission to the data user. The advantages of this model are dynamic, efficient and flexible in terms of access control for outsourced data.

Sujatha Kattimani et al. [22] proposed an ABE (Attribute-Based Encryption) based technique called "A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", which provides efficient security and a high-level framework for accessing the data in Public Cloud. This system includes five substances which address the single-point bottleneck in both security and execution. This method is dynamic in nature and provides much security for data that's shared in the cloud. This multi-authority scheme may be applied in other systems like remote storage system and online common networks, etc. The disadvantage of this scheme is not supporting the flexible delegation of access privileges and shared access privileges.

Shucheng Yu et al. [23] implemented a data access control scheme called "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing". This paper proposed a new mechanism for accessing the data which are stored in Cloud environment with less computational work. This method combines the techniques of ABE, Proxy re-encryption, and lazy re-encryption to achieve the simultaneous fine-graininess, scalability and d ata confidentiality of access control. User access privilege confidentiality and user secret key accountability are the two major features of this scheme. This method enables the data owner to delegate most of the computation-intensive tasks to cloud servers without disclosing any data contents or user access privilege information. In addition to that, it supports user accountability with less extension. The advantage of this scheme is efficient and probably more secure. But it requires heavy computational requests.

The major challenge in sharing data using cloud server is unauthorized cloud service provider and untrusted users. To overcome this Rohit Ahuja et al. [24] proposed a system called "A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing Access Privileges for Cloud Storage." In this system, scalability is achieved by using hierarchical structures of users while providing security using CP-ABE (Ciphertext-Policy Attribute-Based Encryption). The major challenge in incorporating KP-ABE is that the data owner loses control on his outsourced data. Data owner needs to rely on key-issuer to control the access of his outsourced data. To overcome this challenge, data owner is solely responsible for generating and distributing the access privileges among recipients. This method employs five important ingredients to achieve scalability and fine-grained access control and also this extends the feature of CP-ABE.

As cloud computing platform and its services are dynamic in nature, it requires well-defined access control policies and more trusted authentication mechanism for accessing the data. To realize this Syed Rizvi et al. [25] implemented a scheme called "A Semi-Distributed Access Control Management Scheme for Securing Cloud Environment." This paper proposes a new access control mechanism using a Global Resource Management System (GRMS) to effectively deal both local and remote access requests. In addition to this, they used a mechanism called Peered Access Control Module (PACM) and Virtual Resource Manager (VRM) to protect and manage all resources and services of Cloud providers from unauthorized access. In this model, access can be done with minimal request-response time. The disadvantage of this scheme is a

redundancy of checking the policy and procedure to ensure the quality of service.

P.Gutal et al. [26] proposed a system called "Efficient Hierarchical Cloud Storage Data Access Structure with KDC". This system provides authority based data access control policy based on Hierarchical Threshold Access Structure (HTAS) with DKG (Distributed Key Generation). The data access control policy is assigned based on user designation. This system proposed a trusted third party mechanism called Key Distribution Center (KDC) to effectively handle key generation, distribution, and management activities. This system improves the processing time and memory utilization; however, the reliability and security of Key Distribution Center are not addressed properly.

Wang et al. [27] proposed a scheme called "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services". In this paper, they proposed a scheme to ensure confidentiality of data on cloud servers by using HIBE (Hierarchical Identity Based Encryption). This scheme uses the disjunctive normal form policy and generates the keys hierarchically. And this scheme assumed that all attributes in one conjunctive clause are administered by the same domain authority. This scheme ensures high performance, scalability, fine-grained access control and full delegation.

Ensuring data security in data access control is A challenging task in today's Cloud Computing environment. To safeguard sensitive and privacy-relevant data in cloud environment Z.Shen et al. [28] proposed a new provision called "Keyword Search with Access Control over Encrypted Data in Cloud Computing". This model proposed a novel scheme called KSAC which utilizes a recent cryptographic primitive called HPE (Hierarchical Predicate Encryption) to enforce fine-grained access control, perform a multi-field query over encrypted data.

The cloud environment is dynamic in nature, where ensuring data security is very important. To ensure data security in a cloud environment requires an access control mechanism. M.Auxilia et al. [29] introduced a system called "A Semantic-Based Access Control for Ensuring Data Security in Cloud Computing". This system proposes Semantic-Based Access Control model, which ensures interrelationship among different entities in the access control domain. This model considers the semantic relationship among the access control domains such as Subject (user), Object (Data/Resource), Action (select, open, read and write.) The advantage of this model is time and space complexity where access control scheme is enhanced.

Literature study paved a way to know more about data access control techniques in cloud computing environment. Many authors have introduced and implemented various access control systems using different cryptographic techniques. The following table 1 summarizes the functionality of different access control techniques and its limitations.

TABLE I DATA ACCESS CONTROL MODELS AND TECHNIQUES

Access Control methods	Findings	Advantage	Limitations
Mandatory Access Control (MAC)	Multi-layered environment giving access rights to data. Access is allowed when certain constraints are satisfied.	Enforces access control policy based on security levels. Highly secure as it provides multi-level of security. Used in military and government applications.	Low expandability No modification is allowed. Not suitable for all kinds of applications.
Discretionary Access Control (MAC)	Access policies are determined by the owner of the object. It has a mechanism to decide which user can access what resource.	Provides flexibility in the usage of information. Easy to implement and deploy.	Vulnerable to third party attacks. less knowledge regarding the flow of information leads to information loss.
Role Based Access Control (RBAC)	Access is allowed based on the roles of individuals within an organization. Roles are defined according to their position.	Highly flexible, Suited for commercial and enterprise applications. Reduces complexity.	Privileges are assigned based on the role. Updating organization's policy is necessary, to avoid security breaches.
Rule-Based Access Control (RBAC)	Access is allowed based on conditions other than roles. Access decisions are made in real time.	Can be combined with Role Based Access Control to have higher flexibility.	-
Identification Based Access Control (IBAC)	User's identity is required to access system and its resource.	Easy to implement and deploy.	It is not suitable for a larger environment and distributed system.
Attribute-Based Access Control (ABAC)	Access is granted or denied based on attributes of customer and resource. Authentication based access control.	More secure, flexible and scalable. Different encryption techniques are employed with this access model; they are KP-ABE (Key-Policy Attribute-Based Encryption), CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and	Requires a careful analysis of attributes pertaining to the authorization decision.

		HABE (Hierarchical Attribute-Based Encryption).	
Secure, Flexible, Scalable and Fine-grained Access Control	Supports different encryption techniques like Proxy re-encryption, lazy encryption.	Less computational cost Better User revocation policy.	Requires data owner available in online.

III. DATA ACCESS CONTROL MODELS AND TECHNIQUES

Data Access Control is one of the most important technologies to ensure adequate security of cloud computing. There was some traditional access control model which originated in the year of 1970s with the aim to prevent malicious users from accessing resources and avert them to use the potential resources illegally.

Access control mechanisms are a necessary and crucial design element to an application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help to limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Before selecting the data access control mechanisms, there are several fundamental steps that lend a hand speed up and elucidate the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Designing complicated and inconvenient data access controls around uncategorized or non-sensitive data can be counterproductive to the eventual goal or principle of the web application.

2. Determine the relative interaction that data owners and creators have within the web application. Some applications may restrict any and all creations or ownership of data to anyone but not the administrative or built-in system users.

3. Specify the process for granting and revoking user access control rights on the system, whether it is a manual process, automatic upon registration or account creation, or through an administrative front-end tool.

4. Clearly, delineate the types of role driven functions of application support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).

5. Try to align access control mechanisms as close as possible to the organization's security policy. Much of information from the policy can map very well over the carrying out of access control (acceptable time period of certain data access, types of users allowed in seeing certain data or performing certain tasks, etc.). These types of mappings usually work in the most excellent way with Role Based Access Control.

There are a plethora of accepted data access control models in the information security territory. Cloud computing is dynamic in nature and it supports the following traditional Access Control Models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC). Data Access Control actually refers to the control over access to the various system resources after a user's account testimonials and distinctiveness have been legitimated and access to the system approved. For example, a specific user, or group of users, might only be given access to certain files after logging into a system, while simultaneously being deprived of access to all other resources.

A. Discretionary Access Control

Discretionary Access Control (DAC) is used to limit access to information based on the distinctiveness of consumers and/or membership in certain clusters. Access decisions are typically based on the authorizations granted to a user based on the credentials that the owner presented at the time of authentication (username, password, hardware/software token, etc.). Typically in DAC models, the owner of information or any resource is able to change its permissions. The downside of this method is overseer not been able to administer these authorizations on files/information loaded on the web server.

B. Mandatory Access Control

Mandatory Access Control (MAC) is the strictest among all levels of control and is primarily used by the government. MAC takes a hierarchical approach in controlling access to the resources. In this environment, the system administrator has sole responsibility for defining access control to all resource objects such as data files. In this model, security labels are assigned to all resource objects. These security labels contain two kinds of information - a classification (top secret, confidential etc.) and a category (management level, department or project to which the object is available).

When a user requests to access a resource, the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's testament matches the MAC security tag properties, the access is permitted. It is important to note, does both the classification and categories match. A user with top-secret classification, for example, cannot access a resource if they are not only a member in one of the required categories of that object. MAC requires a careful planning to implement. Once it is put into operation, it enforces a high system administration overhead due to necessitate evenly updating of object and accounting labels to have a room for new data, new users and modifications in the categorization and classification of existing users.

C. Role Based Access Control

Another name of this is called as Non-discretionary Access Control and uses real-world approach in structuring access control. Access under RBAC is based on user's profession function within the organization to which the computer system fits in.

Essentially, RBAC assigns special permissions to particular cadres in an organization. For instance, an accountant in a business will be allocated to the Accountant role, achieving access to all the resources legalized for all accountants on the system. Similarly, the developer role can be assigned to software engineer. A user under RBAC may only be assigned a single role in an organization. The accountant illustrated above obtains the same authorizations as all other accountants, nothing more and nothing less.

D. Rule-Based Access Control:

Rules-Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. In this model, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a meticulous account or group endeavors to access a resource, the operating system verifies the rules contained in the ACL for that resource.

Rules-Based Access Control includes conditions such as allowing access to an account or a group to a network connection in certain hours of the day or days of the week. As all access permissions are controlled solely by the system administrator, the user cannot change anything.

IV. SECURITY ISSUES ASSOCIATED WITH THE CLOUD

Cloud computing is a prominent and fast growing technology has captured several professional attentions that allow many to store their data securely and the same can be accessed efficiently. Cloud service provider provides a variety of different service models such as Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service and deployment models as Private, Public, Hybrid, and Community. Nowadays many professionals have started to use cloud environment as it provides the user a storage capability to store and process their data. However, the challenges like data security and access control system are the main concern of Cloud Service provider.

Security concerns associated with cloud computing environment fall into two broad categories: security issues faced by Cloud Service Providers (CSP) (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security issues encountered by their consumers (companies or organizations who host applications or store data on the cloud). However, the responsibility is shared. The Cloud Service Provider must ensure that their infrastructure is secure and that their clients' data and applications are protected with well-defined cryptographic mechanisms, while the user must acquire measures to reinforce their application and apply strong passwords and authentication course.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the sixth biggest threat to cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be repeatedly monitored for mistrustful movement.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers may use Encryption techniques to protect data in the Cloud. The security guidance of Cloud Security Alliance (CSA) recommends data is protected at rest, in motion and in use [30]. Encrypting data avoids illegal accessing of data in Cloud, but it might entail new issues related to access control management [31]. The most three important data security features are data confidentiality, availability, and integrity which prevents data loss].

- Data Confidentiality is a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure.
- Data integrity is the overall completeness, accuracy, and consistency of data. This can be specified by the absence of modification between two instances or between two updates of a data record, meaning data is unbroken and unaffected.
- Data availability is primarily used to create service level agreements (SLA) and similar service contracts, which define and guarantee the service provided by third-party IT service providers.

b) Reasons to Use Secure Cloud Storage and Access Control:

When it comes to storing data in the cloud, it is important to deploy cost-effective technologies and solutions that protect, preserve and manage data to ensure that it is secure, available and accessible when needed.

The cloud, of course, can be a valuable tool in helping IT achieve this objective, but it is important to understand how, where and when cloud services should be used and when they shouldn't. Cloud works best and most cost-effectively when it is part of an overall data management strategy. Because data lifecycles evolve as an organization's data mix changes, you don't want to be locked into using the cloud. Rather, you want to be able to leverage cloud services when appropriate.

Nowadays most of the organizations have started to use public clouds such as Google App Engine (GAE), Amazon Web Services (AWS), IBM Blue Cloud and Windows Azure for storing, managing, processing and accessing their valuable data. The Cloud computing environment proposes diverse services to the user; however, data access service combined with enhanced security mechanism from the cloud plays a vital role. As per the 2017 – State of Cloud Adoption and Security studies, it is observed the following important insights, (i) in another 15 months, 80% of all IT budgets will be committed to Cloud apps and solutions. (ii) There is a tremendous growth in Hybrid cloud adoption, increasing from 19% to 57%. (iii) Public cloud adoption percentage has been improved. (iv) Many organizations today completely trust public clouds to keep their data secure. Public cloud platforms started to invest more for the development and resources in security features and support. To provide better storing and accessing the data in Cloud computing requires advanced data access control techniques and security solutions.

From the survey, the access control model must provide a well strongly controlled data access facility to users and resources with enhanced security mechanism. It must also provide additional capabilities like access control manages user's files and other resources. From the point of access control, (i) cloud computing environment should provide Controlled data access to the various service of the cloud, based on the appropriate access control policies and the level of service requested (or) purchased by the user. (ii) Facilitate proper data access control policy and updated user's information. (iii) Cloud computing supports multitenant environment hence accessing data from one to another requires controlled data access policy. (iv)To ensure better and secure data access service within the cloud environment, there must be a strong relationship between trust and reputation in the data access control models. (v) Providing controlled access to both standard user files and privileged organizational functions. Major stumbling block in cloud computing data access control is a different set of users with diverse sets of enhanced security mechanisms such as storing, managing, processing and accessing of physical resources.

The issues related to data access control in Cloud computing environment can be solved with properly implemented data access control techniques with state-of-the-art security solution and today's implementers can avoid such a issues made by the predecessors

V. CONCLUSION

As per the analysis, it is found that this paper explored various data access control system with adequate security features in cloud computing environment and it is imperative to have efficient, secure, scalable, inter-operability, heterogeneity and a dynamic access control system to get access to the data effectively from the cloud environment. The Continued rise of the Cloud requires highly secured data encryption techniques for accessing the data securely in cloud computing environment and it is highly in need of a good data access control system to access the data as efficiently as possible. Cloud services are influenced by various issues such as data privacy, security and risk management. Understanding all these complexities, it is important to promote high performing data access control mechanism to address the said problems. The future works aim to have a highly secured data storage system and flexible data access policy with less overhead and computation.

REFERENCE

[1] Mell Peter, and Tim Grance, *"The NIST Definition of Cloud Computing."*, pp. 20-23, 2011.

[2] Arockiam, L. and Monikandan, S. and Parthasarathy G. *"Cloud Computing: A Survey"*, International Journal of Internet Computing, Volume 1, No. 2, pp.26-33, 2011.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, *"Plutus: Scalable Secure File Sharing on Untrusted Storage,"* Proc. USENIX Conf. File and Storage Technologies, San Francisco, CA., pp. 29-42, 2003.

[4] H. Lin, Z. Yan and R. Kantola, *"CDController: A Cloud Data Access Control System Based on Reputation,"* IEEE International Conference on Computer and Information Technology (CIT), Helsinki, pp. 223-230,2017.

[5] Chase M., *"Multi-authority Attribute Based Encryption"*, In: Vadhan S.P. (eds) Theory of Cryptography. TCC 2007. Lecture Notes in Computer Science, vol 4392. Springer, Berlin, Heidelberg, 2007.

[6] J. Bethencourt, A. Sahai and B. Waters, *"Ciphertext-Policy Attribute-Based Encryption,"* 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, pp. 321-334, 2007.

[7] X. Liu, Y. Xia, S. Jiang, F. Xia and Y. Wang, *"Hierarchical Attribute-Based Access Control with Authentication for Outsourced Data in Cloud Computing"*, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, pp. 477-484, 2013.

[8] J. Li et al., *"Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing"*, IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, pp. 89-96, 2010.

[9] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. EUROCRYPT' 05, LNCS 3494, Springer, pp. 457-473, 2005.

[10] S. Ruj, A. Nayak and I. Stojmenovic, *"DACC: Distributed Access Control in Clouds"*, IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, , pp. 91-98, 2011.

[11] Z. Yan, X. Li, M. Wang and A. V. Vasilakos, *"Flexible Data Access Control Based on Trust and Reputation in Cloud Computing"*, IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[12] L. Zhou, V. Varadharajan and M. Hitchens, *"Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage"*, IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, 2013, pp. 1947-1960, 2013.

[13] I. El Ghoubach, F. Mrabti and R. Ben Abbou, *"Efficient secure and privacy preserving data access control scheme for multi-authority personal health record systems in cloud computing,"* 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, 2016, pp. 174-179, 2016.

[14] Mustapha Ben Saidi, Anas Abou Elkalam, Abderrahim Marzouk, *"TOrBAC: A Trust Organization Based Access Control Model for Cloud Computing Systems",* International Journal of Soft Computing and Engineering (IJSCE) Volume-2, Issue-4, ISSN: 2231-2307, pp.122-130, 2012.

[15] Dongwan Shin, Ying Wang, and William Claycomb. *"A Policy-based Decentralized Authorization Management Framework for Cloud Computing",* ACM Symposium on Applied Computing (SAC 12), Riva del Garda (Trento), Italy, 26-30, 2012.

[16] S. Fugkeaw and H. Sato, *"CLOUD-CAT: A collaborative access control tool for data outsourced in cloud computing"*, Tenth International Conference on Digital Information Management (ICDIM), Jeju, pp. 243-248, 2015.

[17] M. S. Ferdous, A. Margheri, F. Paci, M. Yang and V. Sassone, *"Decentralised Runtime Monitoring for Access Control Systems in Cloud Federations,"* IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, pp. 2632-2633, 2017.

[18] J. Hu, L. Chen, Y. Wang and S. H. Chen, *"Data Security Access Control Model of Cloud Computing"*, International Conference on Computer Sciences and Applications, Wuhan, pp. 29-34, 2013.

[19] W. Tian, H. Xu, M. Komi and J. Zhang, *"Secure and flexible data sharing via ciphertext retrieval for cloud computing"*, IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), Macau, pp. 161-166, 2017.

[20] F. Khan, H. Li and L. Zhang, *"Owner Specified Excessive Access Control for Attribute Based Encryption,"* in IEEE Access, vol. 4, pp. 8967-8976, 2016.

[21] R. Aluvalu and L. Muddana, *"A dynamic attribute-based risk aware access control model (DA-RAAC) for cloud computing",* IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, pp. 1-5, 2016.

[22] S. Kattimani and S. Pachouly, *"A robust and verifiable threshold multi-authority access control system in public cloud storage"*, 2016 International Conference on Computing Communication Control and automation (ICCUBEA), Pune, pp. 1-4, 2016.

[23] S. Yu, C. Wang, K. Ren and W. Lou, *"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,"* IEEE INFOCOM, San Diego, CA, pp. 1-9, 2010.

[24] R. Ahuja and S. K. Mohanty, *"A Scalable Attribute-Based Access Control Scheme with Flexible Delegation cum Sharing of Access Privileges for Cloud Storage,"* IEEE Transactions on Cloud Computing, vol 14. no. 8, pp. 1-14, 2015.

[25] S. Rizvi and J. Mitchell, *"A Semi-distributed Access Control Management Scheme for Securing Cloud Environment"*, IEEE 8th International Conference on Cloud Computing, New York City, NY, pp. 501-507, 2015.

[26] P. P. Gutal, R. S. Kothe and S. B. Jahveri, *"Efficient hierarchical cloud storage data access structure with KDC",* IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, pp. 328-332, 2016.

[27] Wang, Guojun, Qin Liu, and Jie Wu. *"Hierarchical attribute-based encryption for fine-grained access control in cloud storage services",* 17th ACM conference on Computer and Communications Security,Chicago, Illinois, USA, pp.735-737, 2010.

[28] Z. Shen, J. Shu and W. Xue, *"Keyword search with access control over encrypted data in cloud computing,"* IEEE 22nd International Symposium of Quality of Service (IWQoS), Hong Kong, pp. 87-92, 2014.

[29] M. Auxilia and K. Raja, *"A semantic-based access control for ensuring data security in cloud computing",* International Conference on Radar, Communication and Computing (ICRCC), Tiruvannamalai, pp. 171-175, 2012.

[30] Cloud Security Alliance, *"Security Guidance for critical areas of focus in Cloud Computing V.30,"* CSA, Tech, Rep.,2003.

[31] Arockiam.L. and Monikandan.S, *"Data Security and privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm",* International Journal of Advanced Research in Computer and Communication Engineering, Volume 2.No. 8, pp.3064-3070, 2013.

