IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SECURE AND SCALABLE DATA ACCESS CONTROL IN CLOUD COMPUTING

A Cryptographic Approach

[1]Yash Subhash Kumawat, [2]Prachi Khandelwal, [3]Apoorva Vasishtha
[1]Student, [2] Student, [3]Professor.
[1]JECRC University, Jaipur, Rajasthan, India

Abstract: With its affordable scalability and flexibility, cloud computing has revolutionized data storage. However, it also brings with it serious security risks, especially regarding data access management. While they provide benefits, traditional models like DAC, RBAC, MAC, and ABAC have drawbacks when it comes to protecting data stored in the cloud. To improve security and lessen dependency on data owners, this study suggests a scalable and effective access control framework that combines capability-based access control with an optimized key exchange protocol. We examine the efficacy of current safeguards, discuss major risks to cloud security such data breaches and compliance problems, and offer ways to reduce these dangers. Our results show that the suggested paradigm guarantees safe cloud storage, boosts system performance, and fortifies data safety.

Index Terms **- Cloud Computing, Data Security, Access Control Mechanisms, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), Cryptographic Techniques, Key Management, Data Privacy, Data Integrity, Unauthorized Access, User Authentication, Data Breaches, Access Control Policies, Fine-Grained Access Control, Encryption Techniques, Distributed Systems, Cloud Security Challenges, Cyber Threats and Mitigation, Identity and Access Management (IAM), Compliance and Regulatory Requirements.**

I. INTRODUCTION

Data storage has changed because of cloud computing's scalability, flexibility, and affordability. But it also brings serious security issues, especially regarding data access management. Since illegal access and data breaches continue to be serious risks, it is imperative to guarantee the confidentiality, integrity, and availability of data stored on the cloud. Different degrees of security and flexibility are provided by the conventional access control models of Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Discretionary Access Control (DAC). Although RBAC and DAC offer regulated access, they might not be as flexible in cloud contexts. ABAC allows fine-grained access control but can be computationally costly, while MAC enforces stringent restrictions but is less scalable. This study examines current access control systems and suggests a safe, effective, and scalable architecture that combines dynamic key management with cryptographic approaches. Our method improves cloud security while reducing administrative burden by tackling important issues like compliance, data confidentiality, and authentication.

II. LITERATURE REVIEW

Although cloud computing provides cost-effective and scalable data storage, security, privacy, and access control issues are brought up. This review looks at cloud computing's fine-grained, scalable, and confidentiality-preserving access control systems.

Challenges of Data access Control:

Data management is a hot topic right now because of the rise in data quantities. As organizations begin to shift to the cloud, there is a growing emphasis on ensuring that all information is secure and safe so that there is no chance of information hacking or breaches. Because the cloud enables users to operate without making expensive expenditures on hardware and software, they gain flexibility and data agility. Security, however, becomes a top worry for Cloud owners since the Cloud is frequently shared by several users.

Complex:

Controlling data access may be difficult, especially in large organizations with a variety of people, systems, and data sources. This complexity may make it difficult to develop and maintain an effective data access control system.

Issues with Cloud Security:

A layer of protection from cloud supplier's guards' user's data. However, given how frequently data confidentiality is compromised, it falls short. Phishing, insider, person-in-the-middle, and guessed password attacks are just a few of the various types of assaults that may be made against a target, in addition to assaults from outside sources. The following is a list of safety issues that the cloud currently faces:

Breaches:

There have been instances of cloud security breaches. Hackers have the potential to get through cloud safety precautions and steal data that organizations would otherwise regard as private. In contrast, a breach might be an internal assault, thus companies must closely monitor employee behavior to stop any unintentional attacks on stored information.

Storage:

Organizations can access and virtually store data. However, service providers are required to keep the data within physical infrastructures, making it vulnerable to physical attack. These are a few of the security problems that the cloud environment presents. However, given the degree of technical resources that are now accessible, these can be overcome. To guarantee that it conforms with every regulation and law in addition to the company's internal compliance standards, the greatest safety for the information that is kept is heavily emphasized.

Confidentiality:

The cloud may store a lot of sensitive data. The provider of services or the organization might add more layers of protection to this data to reduce the possibility of leaks and phishing attempts. However, as a precaution, data confidentiality should be given high attention for sensitive information.

Access:

Data security regulations regarding data access and management are essential in the long term. Authorized owners of data are required to allow restricted access to certain people in order to guarantee everyone has only access to the essential parts of the data housed inside the data mart. By restricting and regulating access, several degrees of control and information protection may be implemented to guarantee the maximum level of safety for the stored data.

Integrity:

The system must be configured to provide security and access restrictions. In other words, data should only be accessible to authorized individuals. Data integrity must always be maintained in a cloud environment to avoid any inherent data loss. To avoid a subsequent problem with widespread access, authorization to change the data must be limited as well to a small set of people in addition to access restrictions.

Locality:

It might be challenging to establish the exact position of information storage in the world of clouds because data is typically scattered across several locations. The laws regulating data storage, however, alter when data is moved from one country to another. As a result, data storage in the cloud is subject to compliance difficulties and data privacy legislation. The business must inform users of its data storage policies and the specific location of the information storage server as a supplier of cloud services.

Data Protection and Misuse:

When different organizations utilize cloud computing to store their data, there is often a danger of data misuse. To lessen this danger, information repositories must be protected right away. This operation may be completed using authentication and limited access controls for cloud data.

Opportunities for Data access Control:

Data breaches: If access control is not properly implemented, unauthorized people may be able gain access to sensitive data, which might lead to information theft and the loss of private information. Access control is too stringent: Access control that is too strict can prohibit authorized users from obtaining the information they need to perform their job obligations, which can decrease productivity and anger people. Inconsistency in access control policies can make the administration of access controls difficult and lead to vulnerabilities being introduced into multiple systems.

Access control administration: controlling access control rules and controlling user access may be costly and time-consuming for businesses with several users and data sources. Automating access policies and enforcement is possible with cloud computing. Access control rules may be set up to identify and prevent breaches of security in real-time using machine learning and AI, thus lowering the risk of human mistake and assuring reliable and consistent enforcement of regulations. Greater sensitivity in control of access is made possible by cloud computing, allowing businesses to more precisely manage who has access to what data or resources. By restricting access to just those who require it, this can increase security by lowering the chance of hacking and insider threats.

Scalability: Access control rules may be scaled in the cloud to accommodate different tasks and user groups. For businesses that must handle access for many different people or have varying workloads, this can be very helpful. Access control policies may be maintained centrally using cloud computing, making it simpler to guarantee consistency across various environments and workloads. By eliminating the need for manual intervention and allowing for better monitoring and reporting, this can increase efficiency.

Flexibility: Organizations have more freedom to manage access control rules because of cloud computing. They may pick the model that best suits their needs from a variety of options, including access control based on attributes and role-based access control.

Integration: The use of the cloud opens possibilities for more effective integration with other security tools and technologies, including security analytics platforms, Security Information and Event Management (SIEM) systems, and identity and access management systems. As a result, security problems may be handled more effectively and visibility into control of access events can be improved.

In conclusion, while there are difficulties with limiting access to data in the cloud, there are also chances to increase security and effectiveness by utilizing automation, granularity, scalability, centralized administration, adaptability, and integration. By utilizing these chances, organizations may strengthen their privacy posture and better safeguard their critical data.

III. METHODLOGY

Role-Based Access Controll:

To safeguard data from unauthorized access or change, cloud computing employs several different data access control approaches. These techniques for limiting access to data include: A typical access control method used in cloud computing is role-based access control (RBAC). Users are given roles using RBAC, and depending on those roles, permissions are then given. This makes sure that users only have access to the information and resources they need to do their jobs.

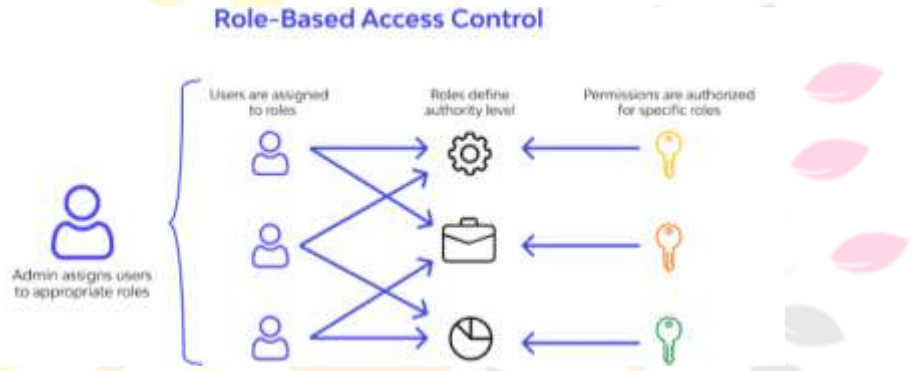

fig. 1

Attribute Based Access Control:

Using factors like a person's ID, the time of day, their location, and the sort of device they are using, Attribute-Based Access Control (ABAC) determines whether someone should have access to a resource. ABAC is very helpful in cloud computing situations where users access resources using various devices and locations.

fig. 2

Mandatory Access Control:

It is a sort of access control that is used to implement a security policy that limits which people or processes have access to a certain resource. In high security settings like government organizations and military locations, MAC is frequently utilized.

fig. 3

Discretionary Access Control:

Users can manage access to their own resources using the Discretionary Access Control (DAC) access control technique. In cloud computing settings where users must share resources with other users, DAC is frequently employed.

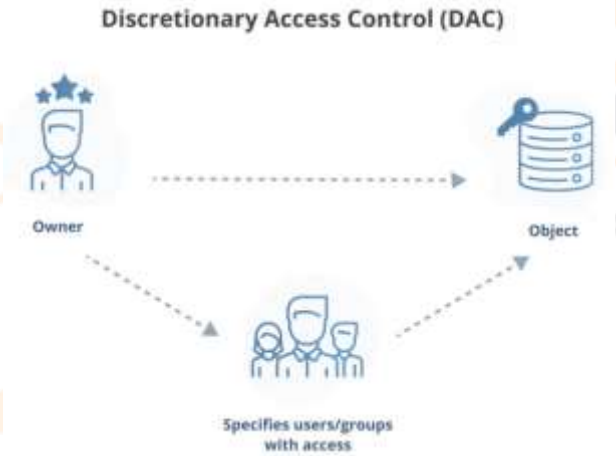

fig. 4

In conclusion, to secure data from unauthorized access or alteration, cloud computing environments utilize a variety of access controls, including RBAC, ABAC, MAC, and DAC. Depending on the security needs of the cloud's setting and the importance of the data being safeguarded, a particular form of access control will be employed.

Classification of Method

1. **Role-Based Access Control (RBAC):**

It is a frequently used access control paradigm that limits system access according to each user's job within an organization. RBAC may be divided into several types, each of which has its own features and advantages.

Because fewer roles need to be generated and maintained, hierarchical RBAC makes roles more logically arranged. This makes managing access privileges easier. Constrained RBAC allows for more precise control over rights of access by limiting what permissions a user may obtain depending on restrictions set on the user's characteristics or the connections between them and the items they are seeking to access.

Dynamic RBAC sets access permissions depending on the user's present context and the state of the system, whereas static RBAC establishes access rights now of assigning roles and remains constant during the user's tenure. Attribute-Based RBAC enables more precise control of access based on a variety of attributes by basing access control choices on the characteristics of the user, the object that is being accessed, and the surroundings in which the request for access is being made.

The framework provided by this material for categorizing RBAC models depending on their features and advantages might be helpful for organizations adopting access control policies since it enables them to select the model that best suits their unique requirements.

2. Attribute-Based Access Control (ABAC):

An access control approach called ABAC (Attribute Based Access Control) uses attributes to decide whether a user is allowed to access a resource or carry out an operation. Organizations can use several types of ABACs to create access control policies, such as:

The subject-based ABAC paradigm allows for limited access depending on a user's role, clearances level, or other qualities by considering the attributes of the person seeking access to a resource.

Resource-depending ABAC: This approach considers the characteristics of the resource that is being used, enabling fine-grained access control depending on the resource's sensitivity, categorization, or other characteristics.

Action-Based ABAC: This model takes the characteristics of what is being requested into account, enabling fine-grained access control depending on the type of action being done, such as read, write, or erase.

Context-depending ABAC: This approach considers the context of the access request, enabling fine-grained access control depending on factors like location, device type, and the time of day.

Organizations may use these ABAC categories to choose the best model for their requirements and put in place access control rules that guarantee privacy and security of their resources.

3. Mandatory Access Control (MAC):

This section discusses the concept of Mandatory Access Control (MAC) as a security policy that applies to all individuals and objects within an information system's perimeter. The main feature of MAC is that it only allows properly designated security administrators, who are trusted subjects, to modify security rules for subjects and objects within the system. Discretionary Access Control (DAC), on the other hand, gives the object owner the discretion to choose which access rights or permissions to provide.

MAC is designed to limit individual choice in granting access and relies on security managers to do so in a more uniform manner. This ensures that the security rules defined for subjects and objects within the system are not easily altered. The owner of the asset has the authority to decide on mandatory access control, but in a more uniform manner with minimal room for the individual choice in who has access.

In practice, MAC is commonly used in government organizations where employees are only permitted access to certain places if they have a specific kind of security clearance, determined by government policy rather than individual authorization. This level of access is determined uniformly, with minimal room for individual choice.

The implementation of MAC also often involves separation of tasks, which limits an individual's work scope and prevents them from accessing information that does not concern them. Another tool that helps this division of duties is role-based access control. Overall, MAC is an important security policy that ensures a uniform level of access control across all individuals and objects within an information system's perimeter.

4. Discretionary Access Control (DAC):

The owner of a resource can manages permissions and access to that resource using the DAC (Discretionary Access Control) access control concept. The following categories can be applied to DAC:

Non-Discretionary DAC: In this approach, access control is managed by an outside party, such as an administrator and is not a discretionary process. The resource owner has no influence over who has access to the resource; access is given in accordance with predetermined guidelines.

Rule-Based DAC: In this approach, actions that are permitted and those that are not permitted are determined by specified rules. The rules are within the resource owner's control, and they may be changed to modify access control policies.

Identity-Based DAC: In this approach, the identity of the person requesting access to the resource serves as the basis for access control. The owner of the resource has control on who has access to it and has the authority to give or deny access based on who the user is.

Access control is dependent on the item being accessed in the object-based DAC paradigm. Depending on the object's attributes, the resource owner can give or revoke access and regulate who has access to the item.

Content-Based DAC: In this paradigm, the content in the resource that is accessed is used to determine how access is granted. Based on information, such as keywords, phrases, or patterns, the person who owns the resource has control over who may access the resource.

These many DAC categories can be helpful for organizations adopting access control policies because they offer a framework for classifying DAC models based on their features and advantages, allowing them to select the model that best suits their unique requirements.

Advantages and Disadvantages

The advantages of Role-Based Access Control (RBAC) include:

It limits access to private data based on the roles and duties of users, improving security by lowering the possibility of unauthorized access or unintentional disclosure of sensitive information.

Access management is made easier thanks to it, which enables centralized control of user access. This reduces the difficulty of keeping different lists of access controls and makes it simpler to grant and revoke rights.

Enhanced productivity: It reduces the need for lengthy approval procedures by allowing users just the essential rights to carry out their tasks. This helps simplify workflows.

Regulation compliance: It ensures that users only have access to the data and systems they need to carry out their job duties, which helps organizations comply with rules.

Its disadvantages include:

Complexity: Setting up it may be difficult, requiring a lot of technical know-how, planning, and resources to guarantee that roles and permissions are applied uniformly throughout the organization.

It can be rigid, which makes it challenging to adapt to changes in roles for users or job duties. Overhead in administration: It calls for continual administration, including role updates as well as access adjustments, which can be labor - and time-intensive.

Risk of mistakes: It can increase the chance of mistakes, such as giving a user the incorrect role or permissions, which might lead to unauthorized access to private information.

It may be a useful access control paradigm overall for businesses trying to increase security and streamline management of access, but it also must be carefully planned, maintained, and properly trained to be used.

Attribute-Based Access Control (ABAC) advantages include:

Granular access control: It enables organizations to build access control rules based on a variety of factors, including user attributes, resource attributes, and environmental attributes. It also gives granular control over access to resources.

Dynamic access control: With the help of it, access choices may be determined in real-time based on the circumstances, the user, and the resource being accessed.

Scalability: Due to its high level of scalability, it is ideal for large, complex organizations with a variety of access control requirements.

Flexibility: It is very adaptable, allowing organizations to set access control rules according to their business needs and the sensitivity of their data.

Its Disadvantages include:

Its implementation may be complicated, requiring a lot of technical know-how, planning, and resources to design the characteristics, policies, and enforcement procedures.

Limited standardization: It is presently not implemented in a standardized manner, which might make it challenging to guarantee compatibility across various systems and suppliers.

An increase in administrative burden is caused by the continual maintenance of attribute definitions and policies, which can take a lot of time and effort.

Error risk: It has the potential for mistakes, such as incorrectly assigning attributes or policies, which might lead to unauthorized access to sensitive data.

In general, it may be a useful access control paradigm for organizations seeking specific control of access and dynamic access choices, but successful deployment and usage of it demands careful design, continuing administration, and efficient training.

(MAC) advantages include:

High security: By implementing rigorous controls on access based on security guidelines set by system administrators, it offers a high level of protection.

It offers centralized control over resource access, making it simpler for administrators to enact rules and regulate access to critical information.

Data confidentiality is preserved with the aid of it, which restricts access to sensitive information to users who have received express permission.

Malware security: It offers malware security by imposing stringent access restrictions and prohibiting unauthorized access to system resources.

Its Disadvantages include:

Limited flexibility: It has a reputation for being rigid, which makes it challenging to adapt to changes in user roles or job duties.

Administrative burden: It needs constant administration, which can be labor- and time-intensive. Examples include administering security rules and access restrictions.

Complexity: Its implementation can be challenging and calls for extensive preparation, financial support, and technical know-how to establish rules and guarantee their uniform application throughout the organization.

lost productivity: If users cannot access the resources, they require to carry out their work duties, it may result in lost productivity.

For organizations seeking to attain a high level of privacy and data confidentiality, it may be a useful access control paradigm overall. However, it also needs careful design, continuing administration, and efficient training to be successfully implemented and used.

(DAC) advantages include:

Flexibility: It is very adaptable and lets users manage who has access to their data and resources.

Simpleness: It is easy to set up and operate, making it suitable for small businesses or those with simple access control needs.

User autonomy: It gives users control over their resources, giving them the flexibility to grant or deny access to others as required.

Reduced administrative burden: Because users oversee controlling access to their own resources, it decreases administrative burden.

Its Disadvantages include:

Limited security: Due to the users' ability to provide access to others regardless of the severity of the material, it only offers a minimal level of protection.

Risk of data leaks: If users allow access to another without the right authority or if their own privacy controls are insufficient, it may increase the risk of data breaches.

Lack of centralized control: Because it lacks centralized management, it is challenging for administrators to manage access rules and keep track of who has access to private information.

Limited scalability: it may be challenging to implement in bigger organizations or in environments with complicated access control requirements.

In general, it can be a straightforward and adaptable access control model for small businesses or those with little access control needs, but it also poses serious threats to data security and might not be appropriate for bigger or more complicated organizations.

Which one is best? MAC, DAC, RBAC or ABAC

It is inaccurate to assert that one access control model is "best" for all organizations because each model has pros and cons of its own and may be more appropriate for a particular type of organization or use case.

For instance, MAC is frequently employed in high security settings where privacy of information is crucial, but DAC may be better suitable for smaller organizations with less demanding access control requirements. RBAC can work effectively for organizations with well-defined roles and responsibilities, whereas ABAC is better suited for big organizations with a variety of access control requirements.

The organization's unique security demands, the sensitivity of the data, and the access control requirements ultimately determine which access control model should be used. It's crucial to thoroughly weigh the benefits and drawbacks of each model before selecting the one that best suits the conditions of your organization.

Uses of Access Controls

Role-based access control (RBAC):

- It is used by big businesses with well-defined roles and responsibilities.
- Healthcare organizations must control patient record access.
- Access to private financial information will be controlled by financial institutions.
- Governmental organizations to control access to sensitive data.

Attribute-based access control (ABAC):

- Massive organizations with a variety of access control needs.
- Environments for cloud computing
- Networks and IoT (Internet of Things) technology gadgets
- Healthcare organizations control access to patient information based on characteristics like department or medical specialty.

Mandatory access control (MAC):

- Military and government organizations must use them to control access to secret information.
- Research labs, nuclear power plants, or financial information centers are examples of high security environments.
- Governmental organizations will control access to very sensitive data.

Discretionary Access Control (DAC):

- Small and medium-sized businesses with less sophisticated access control requirements use.
- Managing student records and course materials access in educational institutions
- Personalized technology, including smartphones and tablets.
- Personal computers and household networks

IV. CONCLUSION

To sum up, access control models like RBAC, ABAC, MAC, and DAC are essential for controlling access to sensitive information and resources in businesses of all sizes and in a range of sectors. Although each model has pros and cons of their own, they all play a vital part in preserving data availability, secrecy, and integrity.

While ABAC is more adaptable and suitable for organizations with a variety of access control requirements, RBAC is best suited for big organizations with well-defined roles and responsibilities. While DAC is easy to set up and wellsuited for smaller organizations with less sophisticated access control requirements, MAC is extremely secure and frequently utilized in high-security situations like military and government organizations.

The final decision about the access control methodology is determined by the unique security demands and access control specifications of each organization. It is crucial to thoroughly weigh the benefits and drawbacks of each model before selecting the one that most closely matches the organization's particular set of circumstances. Organizations may secure the security and safety of their resources and information, safeguard against possible breaches, and ensure compliance with relevant legislation and standards by using efficient access control models.

References

[1] Yu, S., Wang, C., Ren, K., & Lou, W. (2010, March). Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). Ieee.

[2] Yang, K., Jia, X., Ren, K., Zhang, B., & Xie, R. (2013). DAC-MACS: Effective data access control for multiauthority cloud storage systems. IEEE Transactions on Information Forensics and Security, 8(11), 1790-1801.

[3] Peleg, M., Beimel, D., Dori, D., & Dene Kamp, Y. (2008). Situation-based access control: Privacy management via modelling of patient data access scenarios. Journal of Biomedical Informatics, 41(6), 1028-1040.

[4] Namasudra, S. (2021). Data access control in the cloud computing environment for bioinformatics. International Journal of Applied Research in Bioinformatics (IJARB), 11(1), 40-50.

[5] Yan, Z., Li, X., Wang, M., & Vasilakos, A. V. (2015). Flexible data access control based on trust and reputation in cloud computing. IEEE transactions on cloud Computing, 5(3), 485- 498.

[6] Hota, C., Sanka, S., Rajarajan, M., & Nair, S. K. (2011). Capability-based cryptographic data access control in cloud computing. International Journal of Advanced Networking and Applications, 3(3), 1152-1161.

[7] Zhu, Y., Hu, H., Ahn, G. J., Huang, D., & Wang, S. (2012, March). Towards temporal access control in cloud computing. In 2012 Proceedings IEEE Infocom (pp. 2576-2580). IEEE.

[8] Charanya, R., & Aramudhan, M. (2016, February). Survey on access control issues in cloud computing. In 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS) (pp. 1-4). IEEE.

[9] Yu, S., Ren, K., & Lou, W. (2010). FDAC: Toward fine-grained distributed data access control in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 22(4), 673-686.

[10] Yang, K., & Jia, X. (2013). Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE transactions on parallel and distributed systems, 25(7), 1735-1744.

[11] Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Security and Privacy in Communication Networks: 6th International ICST Conference, Secure COMM 2010, Singapore, September 7- 9, 2010. Proceedings 6 (pp. 89-106). Springer Berlin Heidelberg.

[12] Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W., ... & Tang, Y. (2010, November). Fine-grained data access control systems with user accountability in cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 89-96). IEEE.

[13] Markandey, A., Dhamdhere, P., & Gajmal, Y. (2018, September). Data access security in cloud computing: A review. In 2018 International Conference on Computing, Power, and Communication Technologies (GUCON) (pp. 633-636). IEEE.

[14] Namasudra, S., & Roy, P. (2016). Secure and efficient data access control in cloud computing environment: A survey. Multiagent and Grid Systems, 12(2), 69-90.

[15] Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., & Shen, X. (2016). An efficient and fine-grained big data access control scheme with privacy preserving policy. IEEE Internet of Things Journal, 4(2), 563-571