*International Journal of Information Movement* *Vol. 8 Issue X* *(February, 2024)*
*Website: www.ijim.in* *ISSN: 2456-0553 (online)* **Pages 47-54**

# A STUDY OF ACCESS CONTROL AND KEY MANAGEMENT IN THE CLOUD FOR SECURED COMMUNICATION

**Bharti Hasnani**
Ph.D. Research Scholar
Department of Computer Science and Engineering, School of Engineering and Technology,
Raffles University, Neemrana

**Dr. Shiv Kant**
Associate Professor
Department of Computer Science and Engineering, School of Engineering and Technology,
Raffles University, Neemrana
Email-Id: dr.shivkant@rafflesuniversity.edu.in
and
**Dr. Aman Ahmad Ansari**
Associate Professor
Department of Computer Science and Engineering, School of Engineering and Technology,
Raffles University, Neemrana

**Abstract:** Recently, the storage and retrieval of data in the cloud architecture is an attractive research area in cloud computing. Cloud computing has revolutionized the way businesses and individuals store, process, and transmit data. However, the widespread adoption of cloud services has brought about various security challenges, particularly concerning access control and key management. This study provides a comprehensive overview of access control mechanisms and key management strategies in cloud environments to ensure secured communication.the importance of access control in cloud computing, highlighting the need to regulate users' access to resources and data stored in the cloud. Various access control models, including discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC), are discussed. the study explores the significance of effective key management in maintaining data confidentiality and integrity during communication over cloud networks.

**Keywords:** Cloud Computing, Key Management, Access Control, Security, Communication

## 1.0. Introduction

The term "cryptography" describes a simple tool that lets two people communicate across an unsecured channel. These days, the ability to share information inside a group is a standard feature of most communication systems. Instances include data communication, audio and video conferences, information exchange, and other similar applications. Strict security measures are required for group communication. Consequently, protecting the privacy, veracity, and integrity of group messaging is going to be an important issue in the near future. Customers have access to IT infrastructure, including software, hardware, and apps, using web-based technologies known as cloud computing. With cloud computing, users can access cloud-based apps with little to no client-side hardware needed (Indu 2018). Users would be able to access their data from anywhere in the world at any time thanks to the internet and cloud computing.

Cryptographic keys are analogous to safe combinations; we can easily access a safe with the right combination, but it becomes more challenging when we don't. In addition, decrypting encrypted data is easy with the right key but practically impossible without it. Someone could potentially compromise the security of our safe if we are careless with the combination. Similarly, we need to exercise caution when managing the cryptographic keys that we use to encrypt data. Their carelessness will render our encryption security practically useless. Carefully handling keys to prevent their compromise is the essence of key management. There needs to be extreme caution around data loss and theft among cloud service providers and their customers. One of the most fundamental ways that cloud computing systems should protect data is by using strong encryption along with key management. Data encryption for both personal and business use is truly recommended.

**2.0. Cloud Computing Model**

Cloud computing has evolved into a new technology that helps public and private companies save money on computations and get flexible services from Cloud Service Providers (CSPs). In order to protect the privacy, authenticity, and integrity of data stored by third parties, CSP must implement an appropriate access policy. When it comes to enhanced technology, cloud computing is at the forefront. It allows users to pay for access to hardware and software resources. Data migration might be concealed from clients through the use of virtualization, a vital strategy for servicing multi-tenants in resource use. When it comes to handling massively flexible information technology, cloud computing is the way to go. It allows you to provide services to external consumers by utilizing internet resources. A typical model for cloud computing that facilitates the sharing of services via the internet is shown in Figure 1.

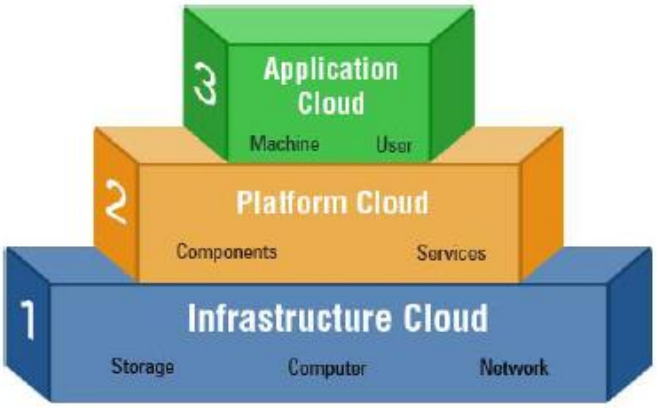


**Figure 1 Cloud Computing Model**

Cloud computing's exponential expansion has supplanted more conventional approaches due to its convenient resource availability, automated tool provisioning, and data configuration on demand. Businesses can rent cloud services and use them fast. Additionally, it offers increased scalability and quick network connectivity for a price. Additional advantages of cloud services include protection against network threats, security controls, and disaster recovery. However, there is a growing need for privacy and security measures to prevent data loss and unauthorized access as cloud computing becomes more widely used. These measures should address concerns related to multi-tenancy, policies, access control, confidentiality, and the preservation of sensitive information.

Despite cloud computing's many advantages, many businesses are hesitant to move their components there. When it comes to cloud data, the most pressing concerns stem from security, privacy, and trust-based risks, which in turn affect the data's accessibility, privacy, protection, location, and secret transfer. When a variety of services are requested from cloud data centers through a traditional network, these risks arise. The data concerns associated with the resource cloud are shown in Figure 2.

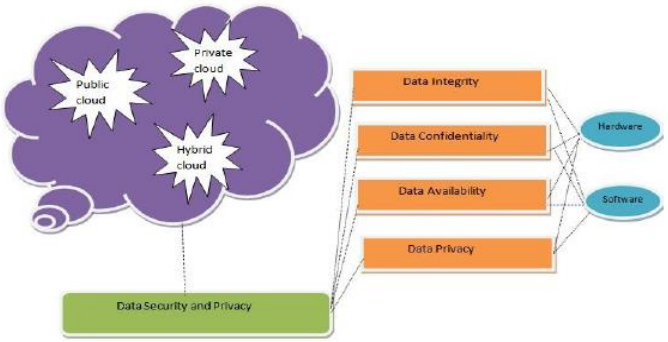


**Figure 2 Data Issues to Cloud**

The term "cloud security" refers to a subfield of information security that deals with the topic of securing data and applications stored in remote data centers, including the introduction of cryptography & explanation of policy and control frameworks. Many cloud clients choose cloud storage services primarily for backup and data recovery. Archive data, rather than user data, is typically created. At the beginning of the project, computation

and resources are measured. At the end of the project, access to them is disabled in order to cut costs.

**3.0. Components Of Cloud**

The widespread availability of resources that no one entity can claim as its own has created a significant demand for cloud computing among major organizations. The capacity to compute constantly changing data that is always available on the cloud is crucial to their expansion. Internet services orientation (SOA), etc., are the technologies that support the cloud. The customer has the option to utilize resources like as memory, CPU, and bandwidth, and can rent cloud storage from the service provider to store most of their data. These five features, together with service and deployment strategies, are what make up a Cloud environment. Part of the cloud's architecture is shown in Figure 3.

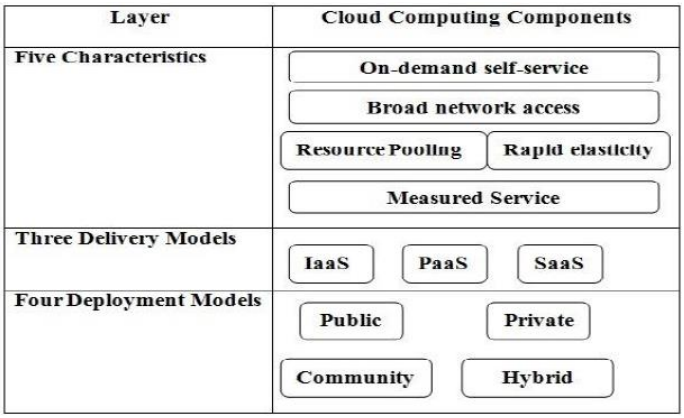


**Figure 3 Cloud Environment Architecture**

The bottom layer of Figure 3 depicts four different deployment models: public, private, communal, and hybrid. On top of that, there are three different deployment methods that leverage different delivery models: SaaS, PaaS, and IaaS. Resource pooling, fast elasticity, metered service, network access, and required services are characteristics of the individual layer that follows this one. A security solution is chosen depending on the deployment model for all of these components.

**4.0 Security In Cloud Computing**

In the cloud computing model, a provider (IaaS, SaaS, or PaaS) builds, launches, and manages the underlying infrastructure, applications, and services. Key elements for making optimum use of current resources and applications are multi-tenancy and virtualization. Through the use of virtualization, numerous users can share a single physical server, data center, computer, and operating system. Through the utilization of shared resources, a cloud provider is able to cater to a substantial user base. Some of the security concerns that arise in a cloud environment as a result of virtualization and multi-tenancy include data protection, communication, and resource management for isolation.

**4.1 Data Security:** At any one moment, numerous users use the same computing infrastructure in the cloud. It is the provider's responsibility to store and handle user data in a shared environment. Any number of malevolent actors could compromise user data. Data privacy and protection in the cloud is becoming more important due to factors such as regulatory concerns with cross-border storage, a lack of transparency on the exact location of cloud storage, and other similar issues. Therefore, important security concerns in cloud computing include data protection, which includes data availability, integrity, and confidentiality.

**4.2 Application Security:** New security concerns arise when software applications are built for or run on cloud computing systems. Any remote-running application must be from a legitimate vendor and free of malware. Application security is at risk due to the cloud's openness, pliability, and public availability. Among the worries is the need to protect the authenticity of programs running on distant servers.

**4.3 Network Security:** The deployment model determines whether a cloud computing is public or private. In a cloud setting, users can access their services and apps from anywhere. Important security challenges include ensuring the continuous availability of cloud services without interruption caused by network security issues such as Denial of Service (DOS) and other types of assaults.

**4.4 Virtualization Security:** New types of assaults against the hypervisor and other parts of the management infrastructure are becoming possible with the advent of virtualization technologies. Virtual servers and

applications cannot be reliably assessed for security. A man-in-the-middle attack can occur during the authorization process for any service in a multi-tenant cloud environment when several virtual machines share the same physical resources. In the cloud, virtual machines can be spun up and rolled back as needed. Consistent security is hard to build and maintain with virtual machines (VMs) since they can be readily moved between physical servers and reverted to earlier instances. Thus, while utilizing cloud resources, there is a risk over virtualization-based security.

**4.5 Identity Management:** Cloud service registration generates identities. A user's identification is used whenever he wants to use a service in the cloud. A big problem with the cloud is unauthorized access to data and programs. A malevolent actor can gain access to a cloud service by pretending to be a genuine user. A service becomes unavailable for normal users when several such hostile organizations get access to cloud resources. The user may also go over their limit while using the service. This may involve gaining entry to a protected region of memory or carrying out any action that is not registered in the Access Control List for that particular application or resource. Therefore, in a cloud computing setting, both providers and users face the challenge of an Identity Management system that provides authentication and authorization. All of these concerns about cloud security are hotspots for new studies and experiments. Cloud security is examined in relation to a number of previously mentioned topics. Network security, data protection, virtualization, resource isolation, and many other related topics are the subject of active investigation. Solutions abound, and more and more are being developed. In this thesis, we look at how one cloud provider handles security concerns for their particular service, and we compare and contrast the different security "trust" approaches they offer.

**5.0 Access Control Techniques In Cloud Computing**

One security approach used to address security vulnerabilities in cloud computing applications is access control policies, which allow, reject, or restrict access to the cloud computing services. It was also the goal of the previous access control methods to detect unauthorized people attempting to enter the network. The security model that Anderson (2010) defines as "Access Control" imposes many restrictions on user behaviors within a system in accordance with the rules specified by the access control mechanism (Wang 2020). The access control view point is illustrated in Figure 4.


Figure 4 Access Control View Point

Some of the most important access control systems are listed here, however there are many more:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

**5.1 Discretionary Access Control (DAC):**Based on the object's capabilities or the user's identification and group membership, the DAC model will offer access to information about the objects to their owners. This permission can be restricted or used to access their own objects. Although DAC is extensively utilized in UNIX-based systems due to its flexibility, it is regarded as the least secure access control technique (Harris, 2002). The path of data access control in the cloud is shown in Figure 5.

**5.2 Mandatory Access Control (MAC):**According to Anderson (2010), the MAC model places the power to grant or deny access to objects and the data contained within them with a centralized authority. Each subject and object is given an access class by MAC so that objects and the information flowing between them can be

securely accessed. To protect data transfer between subjects and objects in a dominance relationship, a security level called an access class is employed. Classifications of objects are security labels that categorize items according to the sensitive information they possess. Subject clearances are a security measure that reflects the reliability or compliance of a subject. In cloud computing, the MAC is shown in Figure 6.

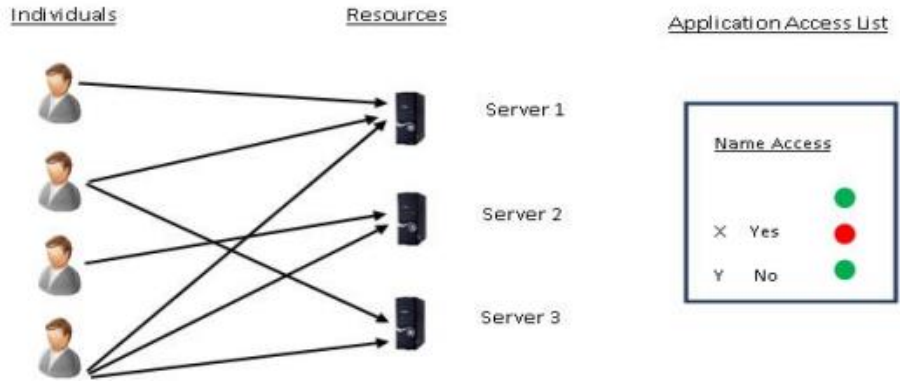


Figure 5 Discretionary Access Control

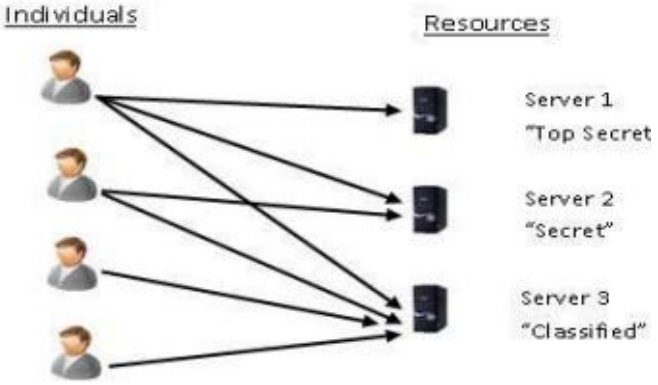


Figure 6 Mandatory Access Control

**5.3 Role-Based Access Control (RBAC):**Roles are used to assign access to objects to users. The functions are defined in relation to how the task is carried out. User roles, and not users themselves, are the focus of every object. In cloud computing, RBAC has a function, as shown in Figure 7.

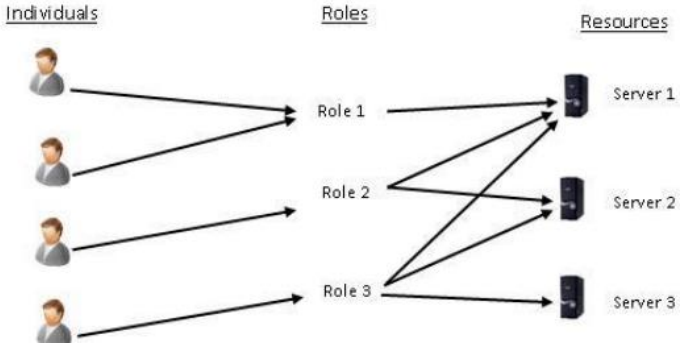


Figure 7 Role-Based Access Control

**6.0 Group Key Management In Cloud Computing**

One of the biggest problems with cloud computing is keeping data secure and making sure users have the appropriate access controls, according to this study. This is especially true as the number of network environments continues to grow. More and more people are relying on cloud services to store and process their own data these days. Ensuring confidentiality and safeguarding the environment during data transmission is crucial, and efficient key management strategies can help with this. For the sake of security and key distribution, this study employs the key agreement method, which calls on every node to produce a unique key and assigns that responsibility to a single node inside the group. Perrig (1999), Steiner et al. (2000), and Kim (2000) are the primary security requirements for this study.

- The leaving member should be denied from accessing the future keys in group – Forward secrecy.
- A new member should be denied from accessing the previous keys in the group – Backward secrecy.
- The keys generated should be absolutely different and independent from the key which was generated previously to avoid prediction – Key independence.

According to Sandro Rafaeli and David Hutchison (2003), there are primarily three types of group key management schemes: distributed, centralized, & decentralized. Group key management taxonomy is displayed in Figure 8.

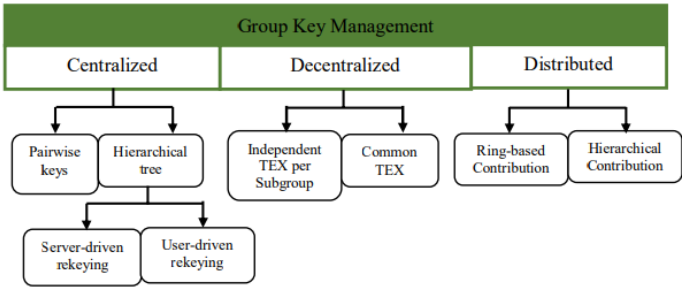


Figure 8 Taxonomy of Group Key Management

**7.0 Cryptography**

Security is the art of encoding information such that it cannot be deciphered. Secret writing is another name for cryptography. Cipher text is an unintelligible version of the original data, such as plain text. With the secret key, you can encrypt data and decrypt it with the same key. Encryption is a branch of mathematics that uses a wide variety of algorithms to protect data.

There are two basic types of cryptography, which is listed as below:

7.1 **Private Key Cryptography**: A type of cryptosystem known as "private key cryptography" uses the same secret key for both encryption and decryption. Secret key encryption is another name for private key cryptography. By utilizing an encryption algorithm & sender's and receiver's shared secret key, private key encryption converts plain text into encrypted text. Using the same decryption process & secret key, the plain text can be acquired. Secret key cryptography is another name for private key cryptography. Both the sender and the receiver in a secret key cryptography transaction use the same key. As an alternative term, symmetric key encryption describes private key cryptography.

7.2 **Public Key Cryptography**: Public key cryptography is a type of cryptosystem that uses two keys—the public key and the private key—to encrypt & decrypt data. A person's private key is their personal secret code that no one else knows. Everyone has a copy of the key, which is called the public key. Public key cryptography also goes by the name asymmetric key cryptography.

The security issues of information encompass the following aspects:

- Confidentiality
- Data integrity
- Availability

**8.0 Encryption And Decryption Techniques**

**8.1 Encryption:** Encryption is one of the most basic security measures utilized in the cloud. The process of transforming readable text into unintelligible cipher text is known as encryption. The secret key, which is exchanged between the sender and the receiver, is used to encrypt the data. Another method of encryption is the symmetric key method. Encrypted files cannot be viewed without the user's knowledge of the decryption key and password. Figure 9 shows both the old and new methods of encryption.

Encryption methods can be broadly classified into two categories:

• Traditional Encryption Techniques
• Modern Encryption Techniques

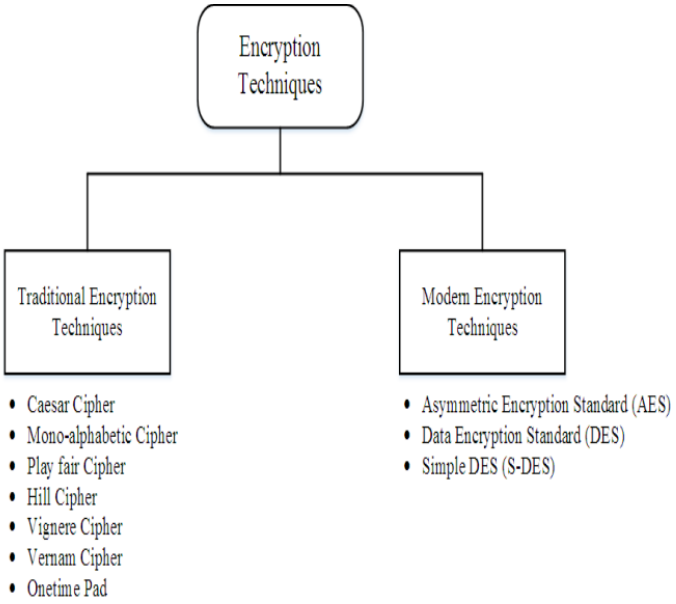


Figure 9 Types of Encryption Techniques

**8.2 Attribute Based Encryption Storage Schemes**

The user and data attributes are the essential components of Attribute-Based Encryption (ABE), which generates keys. Data and policies that are encrypted are described by the characteristics. In the cloud, you can find four main kinds of ABE storage systems, including:

- Key Policy Attribute Based Encryption (KP-ABE)
- Cipher Text Policy Attribute Based Encryption
- Attribute-Based Encryption Scheme with non monotonic Access Structures
- Hierarchical Attribute-Based Encryption

**9.0 Need For Key Management In The Cloud**

Key management, or the practice of overseeing a system's cryptographic keys, entails the following procedures:

- Key Generation
- Key Destruction
- Key Replacement
- Use of Keys
- Key Distribution

**9.1 Issues with Key Management**

Key management in the cloud presents a number of challenges. The following are descriptions of several cloud-related issues: \

- When it comes to cloud platforms, insider attacks are a constant problem. Without the end users' awareness, workers can obtain or steal the keys.
- Every account needs to handle the keys correctly. The task at hand is to efficiently and correctly supply an index with the corresponding keys.
- It is imperative that the key always remain accessible; in the event that the system loses connectivity, the keys must be recovered from cache memory.
- Cached keys are essential for cloud servers because:Byzantine failures are widespread in the cloud and affect many servers. In a Byzantine failure, the server could crash for any number of reasons.
- When an attacker has access to the storage servers in the cloud, they can launch data modification assaults, which are extremely prevalent.

**9.2 Solution to the security issues**

To address the security concerns, we have developed the following solutions:

- Businesses should use cloud encryption if they want to manage their encryption keys covertly.
- It should also safely store the encryption keys off-site.
- Make sure to handle and store the encryption keys in an encrypted manner in many locations.
- Key rotation should be managed properly with new keys, and data should be updated routinely.
- Except for the completion of tasks, employees should not be granted more access.

**9.3 Decryption**

This is basically the opposite of the encryption procedure. It decrypts plaintext using the secret key and ciphertext. Symmetric key cryptography entails encrypting and decrypting with the identical key. Asymmetric key cryptography employs two keys: one for encryption and another for decryption. These keys are mathematically connected.

**10.0 Conclusion**

The study has provided a comprehensive overview of access control and key management in cloud environments, emphasizing their critical role in ensuring secured communication. Through an exploration of various access control models, including DAC, MAC, RBAC, and ABAC, as well as key management strategies such as encryption and cryptographic protocols, the study has underscored the importance of robust security measures to protect sensitive data in the cloud.The integration of access control mechanisms and key management systems within cloud architectures has been highlighted as a fundamental aspect of securing cloud-based communication channels. Further research and advancements in access control mechanisms, key management techniques, and security protocols are necessary to adapt to evolving threats and ensure the continued integrity and confidentiality of data in cloud environments.

**11.0 References**

i. Anilkumar, C., & Sumathy, S. (2018). Security strategies for cloud identity management—A study. *International Journal of Engineering & Technology*, *7*(2), 732-741.
ii. Anilkumar, C., & Sumathy, S. (2018). Security strategies for cloud identity management—A study. *International Journal of Engineering & Technology*, *7*(2), 732-741.
iii. Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2019). Survey of access control models and technologies for cloud computing. *Cluster Computing*, *22*, 6111-6122.
iv. Chandramouli, R., Iorga, M., & Chokhani, S. (2013). Cryptographic key management issues and challenges in cloud services. *Secure Cloud Computing*, 1-30.
v. Harris Wang 2002, 'An Access Control Scheme for Web-Based ELearning Systems', 7th International Conference on Information Technology Based Higher Education and Training, Ultimo, NSW, Australia, ITHET '06, pp.1-6.
vi. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, *21*(4), 574-588.
vii. Kim, Y, Perrig, A & Tsudik, G 2000, 'Simple and fault-tolerant key agreement for dynamic collaborative groups', Proceedings of the 7th ACM conference on Computer and communications security (CCS00), pp. 235–24
viii. Oruganti, R., & Churi, P. (2022). Systematic survey on cryptographic methods used for key management in cloud computing. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 2* (pp. 445-460). Springer Singapore.
ix. Perrig, A 1999, 'Efficient collaborative key management protocols for secure autonomous group communication', International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC' 99), pp. 1-11.
x. Rasseena, M., & Harikrishnan, G. R. (2014). Secure Sharing of Data over Cloud Computing using Different Encryption Schemes An overview. *International Journal of Computing and Technology, Volume1*, (2), 8-11.
xi. Sandro Rafaeli & David Hutchison 2003, 'A Survey of Key Management for Secure Group Communication', ACM Computing Surveys, Vol. 35, No. 3, pp. 309–329.
xii. Steiner, M, Tsudik, G & Waidner, M 2000, 'Key agreement in dynamic peer groups', IEEE Transactions on Parallel and Distributed Systems, Vol.11, No. 8, pp. 769–780.
**xiii.** Wang, H., Cao, J., & Zhang, Y. (2020). *Access Control Management in Cloud Environments* (pp. 3-297). Springer.