**CHAPTER-3**

**EXISTING SYSTEM**

* In existing systems, data sharing in clouds often involves using encryption techniques to protect sensitive data. Attribute-based encryption (ABE) is a popular technique that allows users to encrypt data based on specific attributes, such as age, gender, or job title, rather than individual identities. This enables flexible and efficient data sharing while maintaining data privacy.
* However, in ABE systems, there are often challenges in terms of key management and revocation. When a user's attributes change, their access to encrypted data needs to be updated accordingly. This can be a complex and time-consuming process, particularly when there are many users and large amounts of data involved.
* Proxy re-encryption (PRE) is a technique that can be used to address some of the key management and revocation challenges in ABE systems. PRE allows a trusted third party, known as a proxy, to re-encrypt data without accessing its plaintext content. This enables efficient and flexible key management and revocation, as the proxy can simply re-encrypt data for users based on their updated attributes.
* However, existing PRE schemes do not always provide verifiability and fairness, which are important properties for data sharing in clouds. Verifiability ensures that users can check that their data has been properly re-encrypted and that the proxy has not tampered with it. Fairness ensures that users with the same attributes are treated equally in terms of access to the encrypted data.

**DISADVANTAGES**

Some potential disadvantages of a Verifiable and Fair Attribute-based Proxy Re-encryption Scheme for Data Sharing in Clouds include:

Complexity: Developing and implementing such a scheme can be complex, particularly when dealing with large amounts of data and many users with different attributes. This can make it difficult to ensure the scheme is secure and efficient.

Trust in the proxy: A trusted third party, or proxy, is required to perform the re-encryption. Users must trust the proxy to perform this task properly and not tamper with their data. If the proxy is compromised, it could result in a data breach or unauthorized access to sensitive information.

Key management and revocation: While the use of PRE can simplify key management and revocation, it can still be a complex process. Ensuring that user access to data is properly updated when their attributes change, or when they are removed from the system, can be challenging and may require significant administrative resources.

Overhead: The use of ABE and PRE techniques can introduce additional overhead in terms of computation and communication, particularly when dealing with large amounts of data. This could impact the performance and scalability of the system.

Compatibility: Existing systems and applications may not be compatible with the Verifiable and Fair Attribute-based Proxy Re-encryption Scheme, requiring modifications or the use of additional tools and resources to ensure compatibility.