**2.1 INTRODUCTION:**

In recent years, cloud computing has grown from a small concept to a rapidly growing part of IT industries. It enables numerous people to share information without geographical restrictions. Therefore, protecting sensitive files stored in the clouds from being tampered by malicious attackers is essential to the success of the clouds. Nowadays, data security has become a critical issue in various kinds of applications. Users may prefer storing their files in an encrypted manner and delegating decryption rights efficiently. In order to protect the files stored in the clouds, the owners can encrypt the files by using their keys before uploading the files to the clouds. Still, a user needs to be online to share her encrypted files because she needs to send her keys to her friends. It is extremely inefficient because of the heavy overhead on the user. Fortunately, proxy re-encryption(PRE) schemes ,enable users to share their encrypted files with other users by using re-encryption keys

Cloud computing is emerging as a viable option for internet based development and services. Cloud computing is a distributed computing paradigm where the computing resources such as hardware, software, processing power are delivered as a service over a network. The cloud computing model allows the users to access information and computer resources from anywhere that a network connection is available.

Cloud computing aims to provide reliable, customized, and quality of service (QoS) guaranteed dynamic computing environments for end-users. However, there are applications such as e-health and emergency response monitoring that require quick response and low latency. Delays caused by transferring data over the cloud can seriously affect the performance and reliability of real-time applications. Before outsourcing e-health care data to the cloud, the user needs to perform encryption on these sensitive data to ensure its confidentiality. Conventionally, any modification to the user data requires encrypting the entire data and calculating the hash of the data from scratch. This data modification mechanism increases communication and computation costs over the cloud.

**2.5 LITERTURE SERVERY:**

**TITLE:** Type Based Proxy Re-encryption Scheme

**AUTHOR:** Lwanga Newton

**Description:**

Type based proxy re-encryption scheme are proposed by Tang [21]. This encryption scheme guarantees data confidentiality and fine gain access control. Type based proxy re-encryption enables the delegator to implement fine grained policies with one key pair without any additional trust on the proxy. In this scheme the delegator categorizes his ciphertexts into different subsets. Then the decryption right of each subset is delegated to a specific delegate. The ciphertexts for the delegator are generated based on the delegator’s public key and the message type which is used to identify the message subset. The type based PRE has the following properties. 1. The delegator only needs one key pair so that key management problem can be simplified. 2. The delegator can choose a particular proxy for a specific delegate, which might be based on the sensitiveness of the delegation. Compromise of one proxy key will only affect one subset of messages.

**TITLE:** Key Private Proxy Re-encryption Scheme

**AUTHOR:** Amanze Bethran Chibuike

**DESCRIPTION:**

Key private proxy re-encryption scheme are proposed by Ateniese et al. [5]. In a key private PRE it is impossible for the proxy and a set of colluding users to derive the recipient of a message from the ciphertext and the set of public keys. Achieving key private PRE is only possible when the underlying encryption scheme is key-private. The key privacy encryption provides privacy of the key under which the encryption was performed [17]. The KP-PRE scheme formulates the notion of keyprivacy for proxy re-encryption schemes, where even the proxy which performs the translations cannot able to distinguish the identities of the participating parties. In addition to hide the contents of files from the proxy, it is also useful to suppress as much meta-data as possible. For example, we might want the proxy file server to re-encrypt sensitive files for certain recipients without the proxy the recipient’s identity.

**TITLE:** Identity Based Proxy Re-encryption Scheme

**AUTHOR:** Feras Al-hawari

**DESCRIPTION:**

The identity based PRE scheme was introduced by Shamir [22]. In an identity based PRE scheme, arbitrary strings such as email addresses or IP address can be used to form public keys for users. In identity based encryption, the senders encrypt messages using the recipient’s identity (a string) as the public key. For instance, Alice could encrypt a message for Bob by just using his email address [15]. The identity based proxy re-encryption schemes allow a proxy to translate an encryption under Bob’s identity into one computed under Alice’s identity. The proxy uses proxy keys, or re-encryption keys, to perform the translation without being able to learn the plaintext. The identity based proxy re-encryption [4] ensures that no reasonable set of colluding key holders will obtain an advantage against non-colluding users. The IBE has a number of practical applications such as secure email forwarding, attribute-based delegations and access control in networked file storage. This type of re-encryption schemes is used to realize the secrecy of data.

**TITLE:** Attribute Based Proxy Re-encryption Scheme

**AUTHOR:** Yongqiang He

**Description:**

The concept of attribute based PRE was introduced by Sahai and Waters [2]. In attribute based proxy re-encryption scheme, a semi trusted proxy with some additional information can transform a ciphertext under a set of attributes into a new ciphertext under a set of attributes into a new ciphertext under another set of attributes on the same message. This encryption scheme, allows fine-grained access control on encrypted data. Attribute based encryption is a generalization of IBE. The data provider can express how he wants to share data in the encryption algorithm itself. Goyal et al. [9] introduced two variants of attribute based encryption (ABE) namely ciphertext policy attribute based encryption (CP-ABE) and key policy attribute based encryption (KP-ABE). In a CP-ABE scheme, a user’s private key is associated with a set of attributes and an encrypted ciphertext will specify an access policy over attributes. In KP-ABE [9] scheme, each ciphertext is labelled by the encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt. An important aspect of KP-PRE scheme deals with secure forensic analysis. In ABE technique, the data is stored on the storage server in an encrypted form while different users are still allowed to decrypt different pieces of data as per security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access.

**TITLE:** Conditional Proxy Re-encryption Scheme

**AUTHOR:** A.S.Misal

**DESCRIPTION:**

The Conditional proxy re-encryption (C-PRE) was introduced by Jean Weng and others [12]. The C-PRE scheme involves three principles: a delegator (Ui), a proxy and a delegate (Uj). A message sent to delegator Ui with condition w is encrypted by the sender using both Ui’s public key and w. To re-encrypt the message to Uj the proxy is given the re-encryption key (rki→ j) and the condition key (cki , w) corresponding to w. Both the keys can be generated only by ui. These two keys form the secret trapdoor used by the proxy to perform ciphertext translation. The proxy is unable to translate those ciphertext whose corresponding condition keys are not available. Therefore, Ui has a flexible control on delegation by releasing condition keys properly. This PRE scheme works in practice as follows: the message encrypted for Ui is first handled by proxy transforms the ciphertext into a ciphertext for Uj . However, proxy will obtain no information about the original message. The security requirements for C-PRE systems should ensure that, (i) even if the proxy, who does not have both the partial re-encryption key and the condition key, colludes with the delegate, it is still impossible for them to compromise the delegator’s security. (ii) The proxy, who has both the partial reencryption key and the condition key, compromises neither the delegator not the delegatee’s security.