**EXISTING SYSTEM**

Over time, in healthcare, electronic health records (EHR) have replaced the paper record system, so that data can be handled and maintained efficiently. It further improves the availability, sharing, and cost of data maintenance. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used to provide security and access control in cloud

Risk problems become even more critical as IoT devices share sensitive data because they are directly connected to the Internet.

However, many existing schemes for secure data sharing and communication in cloud computing have limitations, i.e., delays between user requests and responses from the cloud due to a drastic increase in data volume. A large number of users are involved in outsourcing and cryptographic operations.

* Collusion problem and Plaintext attack
* The key privacy proof is more difficult than that of CPA security
* Requires effective time period to be the same for all attributes associated with the user

**DISADVANTAGES**

• It is time consuming

• It lacks of data security

• Retrieval of data takes lot of time

• Percentage of accuracy is less