**CHAPTER 3**

**EXISTING SYSTEM**

* Despite its superiority in data sharing, the public key searchable encryption mechanism suffers from various attacks when being deployed in cloud storage, and may lead to privacy leakage.
* A cloud server cannot learn any information about a newly added encrypted data file containing the keyword that previously queried.

**DISADVANTAGES**

* The only disadvantage of **public** **key** **encryption** is a **key** distribution problem: if you need to verify/check your file by multiple software instances, i.e., you're signing an upgrade patch, it's a problem to pass your **key** untampered to the clients, so forging/MitM will be impossible.