**EXISTING SYSTEM:**

In order to enable end-users to control the access of their own data stored on untrusted remote servers (e.g., cloud servers), encryption-based access control is an effective method, where data are encrypted by end-users and only authorized users are given decryption keys. This can also prevent the data security during the transmission over wireless networks which are vulnerable to many threats . However, traditional public key encryption methods are not suitable for data encryption because it may produce multiple copies of ciphertext for the same data when there are many data consumers in the system. In order to cope with this issue, some attribute-based access control schemes are proposed by leveraging attribute-based encryption which only produces one copy of ciphertext for each data and does not need to know how many intended data consumers during the data encryption. Moreover, once the cloud data are encrypted, some searchable encryption algorithms are proposed to support search on encrypted cloud data.

**DISADVANTAGES:**

* Existing methods which only partially hide the attribute values in the access policies
* End-users may worry that the cloud server may make wrong access decision intentionally or unintentionally, and disclose their data to some unauthorized users.
* Attribute-based access control schemes can deal with the attribute revocation problem , they all suffer from one problem: the access policy may leak privacy. This is because the access policy is associated with the encrypted data in plaintext form.

**PROPOSED SYSTEM:**

1. We propose an efficient and fine-gained big data access control scheme with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes.

2) We also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

3) We further give the security proof and performance evaluation of our proposed scheme, which demonstrate that our scheme can preserve the privacy from any LSSS access policy without employing much overhead.

**ADVANTAGES:**

* we have proposed an efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information.
* our method can hide the whole attribute (rather than only its values) in the access policies
* our scheme is selectively secure against chosen plaintext attacks.