**CHAPTER-2**

**INTRODUCTION**

Cloud computing, which provides adequate storage and computation capability, has been a prevalent information infrastructure. Instead of managing data locally, cloud services provide an opportunity for users outsourcing their data on the cloud without data management concerns. While it is so convenient to use, data security and privacy especially access control on shared data become a concern since the cloud service is usually provided by third parties such as the Amazon cloud services and Alibaba cloud. Recently, attribute-based encryption (ABE) has been adopted to support flexible access control on user’s credential. In a typical ABE scheme, a user’s credential and ciphertext are associate with an attribute set and an access policy. The ciphertext can only be decrypted when the attribute set satisfies the access policy. However, ABE lacks the ability of encrypted data sharing which is critical in the situation of collaboration needed

**LITERATURE SURVEY**

# 1. Title: Security Challenges for the Public Cloud

**Author**: Cong Wang

**ABSTRACT**:Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

**2.Title:** Fuzzy Identity-Based Encryption

**Author**:Brent Waters

**ABSTRACT**

# We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, *ω*, to decrypt a ciphertext encrypted with an identity, *ω* ′, if and only if the identities *ω* and *ω* ′ are close to each other as measured by the “set overlap” distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled.

# 3.Title:Attribute-based encryption with verifiable outsourced decryption

**Author:** C Guan

**ABSTRACT:**

Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows  
users to encrypt and decrypt data based on user attributes. A promising application of ABE is  
flexible access control of encrypted data stored in the cloud, using access polices and  
ascribed attributes associated with private keys and ciphertexts. One of the main efficiency  
drawbacks of the existing ABE schemes is that decryption involves expensive pairing  
operations and the number of such operations grows with the complexity of the access.

# 4.Title:Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing

# Author:R Zhang

# ABSTRACT:

# We propose two ciphertext-policy attribute-based key encapsulation mechanism (CP-AB- KEM) schemes that for the first time achieve both outsourced encryption and outsourced decryption in two system storage models and give corresponding security analysis. In our schemes, heavy computations are outsourced to Encryption Service Providers (ESPs) or Decryption Service Providers (DSPs), leaving only one modular exponentiation computation for the sender or the receiver.

# 5.Title:Ciphertext-policy attribute-based encryption

**Author**:J Bethencourts

**ABSTRACT:**

In several distributed systems a user should only be able to access data if a user posses a  
certain set of credentials or attributes. Currently, the only method for enforcing such policies  
is to employ a trusted server to store the data and mediate access control. However, if any  
server storing the data is compromised, then the confidentiality of the data will be  
compromised