**CHAPTER-2**

**INTRODUCTION**

Cloud storage has become a promising paradigm with the explosive growth of data in recent years. It not only provides an on-demand storage service for users, but also facilitates users’ access to data. However, data outsourced to cloud server may contain some sensitive information (e.g., company financial data, health records), which may incur security and privacy issues. To protect data confidentiality, one general approach is to encrypt the data before transferring it to the cloud server. But the encrypted data makes its utilization more difficult, particularly the ability of data retrieval. To implement the searchable feature of encrypted data, Song et al. [1] were the first to propose the notion of searchable encryption (SE) based on the symmetric crypto-system. Subsequently, to avoid the key management and distribution, Boneh et al. [2] introduced the notion of public-key encryption with keyword search (PEKS) and constructed a concrete scheme based on the asymmetric crypto-system. Under the PEKS framework, there are three entities namely, the data owner, the data receiver (user) and the cloud server. Using the public key of the data receiver, the data owner encrypts the files and each keyword which is extracted from these files, and then uploads the ciphertexts to the cloud server. The data user sends a trapdoor containing the keyword which he/she wants to search to the cloud server. The cloud server tests whether the keyword in corresponding to the trapdoor is equal to the keyword underlying the ciphertext. The cloud server returns the encrypted data corresponding to the trapdoor. Fig.1 describes the process.

**LITERATURE SURVEY**

### Title: [Practical techniques for searches on encrypted data](https://ieeexplore.ieee.org/abstract/document/848445/)

### Author: DX.Song

# Abstract: It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide.

### Title: [Public key encryption with keyword search](https://link.springer.com/chapter/10.1007/978-3-540-24676-3_30)

# Author: [Giuseppe Persiano](https://link.springer.com/chapter/10.1007/978-3-540-24676-3_30#auth-Giuseppe-Persiano)

# Abstract: We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice’s public key. An email gateway wants to test whether the email contains the keyword “urgent” so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word “urgent” is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others.

### Title: [Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack](https://ieeexplore.ieee.org/abstract/document/6296654/)

### Author:P Xu

# Abstract: Public-key encryption with keyword search (PEKS) is a versatile tool. It allows a third party knowing the search trapdoor of a keyword to search encrypted documents containing that keyword without decrypting the documents or knowing the keyword. However, it is shown that the keyword will be compromised by a malicious third party under a keyword guess attack (KGA) if the keyword space is in a polynomial size. We address this problem with a keyword privacy enhanced variant of PEKS referred to as public-key encryption with fuzzy.

### Title: [A new general framework for secure public key encryption with keyword search](https://link.springer.com/chapter/10.1007/978-3-319-19962-7_4)

# Author: P Chen

# Abstract: Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in *Eurocrypt’04*, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted servers, as long as they do not collude. We then present a generic construction of DS-PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), which is of independent interest.

### Title: [Practical techniques for searches on encrypted data](https://ieeexplore.ieee.org/abstract/document/848445/)

**Author**: DX Song

# Abstract: It is desirable to store data on data storage servers such as mail servers and file server sin encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide