

# DESIGN AND ANALYSIS OF A SEARCHABLE SYMMETRIC KEY CIPHER SYSTEM

By:  
Asanka Balasooriya  
Kelum Senanayake

# SECURITY REQUIREMENTS

A cryptographic scheme which enables searching on encrypted data without revealing to the server should have following features.

- Untrusted server should not be able to learn anything about the plaintext given only the ciphertext
- Untrusted server should not be able to search for a word without authorization of the client
- The scheme should be efficient and practical



# THE PROPOSED SCHEME

Let's assume that Alice is the client who owns important data and wants to store in Bob's cloud storage which is untrusted.

The scheme is as follows;

- Alice builds an index with keywords that Alice may want to search for later for all data currently she owns.
- Then she encrypts all the plain data using a symmetric encryption key.
- All the keywords of the index are encrypted using the same key.
- Lists of positions of the index are left as plain data.
- Store the complete index and ciphertext of the plain data on Bob's server.



Let's assume the selected encryption mechanism is **E** with a key ***k***.

- The list of plaintexts of Alice =  $\{P1, P2, P3 \dots Pn\}$
- Corresponding ciphertexts =  $\{C1, C2, C3, \dots Cn\}$
- The set of selected keywords of the index =  $\{w1, w2, w3 \dots wm\}$
- Then the index with encrypted keywords is as follows for a keyword ***wi***
- $E_k(wi) \text{ -----}>> \{Cp, Cq, Cr, \dots Ct\}$



# SEARCHING FOR A SPECIFIC KEYWORD $W_J$ IS AS FOLLOWS

- Alice computes  $E_k(\mathbf{w}_j)$  value and send it to Bob.
- Bob searches the index entries for  $E_k(\mathbf{w}_j)$  and finds a match.
- Bob reads the list of positions associated with encrypted keyword sent by Alice for the search in the index.
- Bob sends the list of ciphertexts fetching using the list of positions to the Alice as the search result.
- Alice decrypts ciphertexts to access the corresponding plaintexts.



# SECURITY STRENGTHS OF THE SCHEME

- Bob is unable to identify the content of the data since both data and keywords are encrypted.
- The proposed scheme provides controlled searching where Bob is not be able to search without the authorization of Alice
- Bob knows nothing more than the encrypted search result for an encrypted keyword if he tries to do a search which is not asked by Alice




# SECURITY ATTACKS

Basically statistical attacks can be done on this scheme in two ways.

- Bob may statistically analyze the index to identify certain keywords. Although the keywords are encrypted, Bob still is able to identify most common words which are associated with large set of documents.
- Bob may observe number of search requests and statistically identify access patterns of Alice.



# SOLUTIONS

- Statistical attacks on index can be prevented by maintaining lists of document positions for keywords in fixed size lists. For words that appear infrequently, Alice can pad the list to the fixed size. For more common words, Alice can split the long list into several lists with the fixed size. Then to search for such a word, Alice will need to ask Bob to perform and merge several search queries in parallel.
  - The second kind of attacks is hard to avoid unless performing several unwanted searches together with regular searches. This way Bob can be misled to identify false access patterns.
- 



# WEAKNESSES OF THE SCHEME

- Alice must update the index whenever she changes her documents.
- Ideal for read only data storages.
- Bob might be able to learn through updating the index.
  - If Alice does not change the index for a key word when she adds a new document to the server, then Bob is able to know that the keyword is not included in the newly created document.
  - Alice must update substantial part of the index to hide real updates.



# REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *IEEE Symposium on Security and Privacy*, 2000.

[2] Changyu Dong, Giovanni Russello and Naranker Dulay. No Shared Keys: Multi-user Searchable Data Encryption. Department of Computing, Imperial College London.



THANK YOU

