

What is claimed is :

1. A system for creating a privacy enhanced personal search index, the system comprising:

at least one processor; and

memory coupled to the at least one processor, the memory comprising computer executable instructions that, when executed by the at least one processor, perform a method comprising:

at a server, receiving an encrypted opaque document digest from a client device, wherein the encrypted opaque document digest is associated with a user;

at the server, receiving an index key from the client device;

at the server, decrypting the encrypted opaque document digest with the index key;

at the server, indexing the decrypted opaque document digest; and

at the server, creating a user-specific opaque search index using the indexed decrypted opaque document digest, wherein the user-specific opaque search

index is personal to the user; and wherein authorized access to the user-specific opaque search index is restricted to the user.

2. The system of claim 1, wherein the method further comprises receiving an encrypted document.

3. The system of claim 2, wherein the decrypted opaque document digest comprises one or more opaque terms and opaque metadata describing the encrypted document.

4. The system of claim 3, wherein the decrypted opaque document digest further comprises document snippets from the encrypted document, wherein the document snippets comprise at least one of:

a summary of the encrypted document;

metadata associated with the encrypted document; and

one or more sentences from the encrypted document.

5. The system of claim 1, wherein a transformation key is used to convert the decrypted opaque document digest to a cleartext document digest.
6. The system of claim 5, wherein the transformation key is not accessible by the system.
7. The system of claim 1, wherein the system is a partially trusted environment, wherein cleartext data associated with the decrypted opaque document digest remains opaque in the partially trusted environment.
8. A system for searching a privacy enhanced personal search index, the system comprising:
- at least one processor; and
 - memory coupled to the at least one processor, the memory comprising computer executable instructions that, when executed by the at least one processor, perform a method comprising:
 - at a server device, receiving an opaque query digest from a client device, comprising at least one opaque term associated with a user;
 - at the server, receiving an index key from the client device;
 - at the server, decrypting the encrypted opaque document digest with the index key;
 - at the server, indexing the decrypted opaque document digest; and
 - at the server, creating a user-specific opaque search index using the indexed decrypted opaque document digest, wherein the user-specific opaque search index is personal to the user; and wherein authorized access to the user-specific opaque search index is restricted to the user;
 - identifying the at least one opaque term in the user-specific opaque search index;
 - retrieving query results from the user-specific opaque search index;
 - ranking the query results according to a relevance of the at least one opaque term to create ranked query results; and
 - transmitting the ranked query results to a processing device associated with the user.

9. The system of claim 8, wherein the method further comprises:
- using the query results, retrieving an encrypted document from a data store; and
- transmitting the encrypted document to the processing device.
10. The system of claim 9, wherein the system is a partially trusted environment, wherein cleartext data associated with the opaque query digest, the query results and the encrypted document remains opaque in the partially trusted environment.
11. The system of claim 9, wherein the query results comprise at least an opaque document name, wherein the at least opaque document name is provided to a storage management utility that retrieves the encrypted document from the data store.
12. The system of claim 8, wherein the query results comprise:
- the at least one opaque index term; and
- at least one document snippet from at least one of a plurality of encrypted documents.
13. The system of claim 8, wherein the opaque query digest comprises one or more opaque terms and opaque metadata describing a query.
14. The system of claim 13, wherein a transform key was applied to a cleartext query digest to create the opaque query digest.
15. The system of claim 14, wherein an index key was applied to the cleartext query digest to create the opaque query digest.
16. A method for searching a privacy enhanced personal search index, the method comprising :
- at a server, receiving an encrypted opaque document digest from a client device, wherein the encrypted opaque document digest is associated with a user ;

at the server, receiving an index key from the client device;

at the server, decrypting the encrypted opaque document digest with the index key ;

at the server, indexing the decrypted opaque document digest; and

at the server, creating a user-specific opaque search index using the indexed decrypted opaque document digest, wherein the user-specific opaque search index is personal to the user, and wherein authorized access to the user-specific opaque search index is restricted to the user;

at a server, receiving an opaque query digest, wherein the opaque query digest comprises one or more opaque terms associated with a query;

searching the user-specific opaque search index using the at least one opaque index term, wherein the user-specific opaque search index is personal to the user; and

wherein authorized access to the user-specific opaque search index is restricted to the user;

upon identifying the at least one opaque index term in the user-specific opaque search index, retrieving query results from the user-specific opaque search index;

ranking the query results according to a relevance of the at least one opaque term to create ranked query results; and

transmitting the ranked query results to the client device.

17. The method of claim 16, wherein the client device executes a trusted environment that is configured to expose cleartext data associated with the ranked query results and the encrypted document.

18. The method of claim 16, wherein the user-specific opaque search index comprises information identifying an encrypted document and at least one of the one or more opaque terms associated with the query.

19. The method of claim 16, the method further comprising:

searching a data store using the at least one opaque index term;

upon identifying the at least one opaque index term in the data store, retrieving an encrypted document associated with the at least one opaque index term, wherein a document key was applied to a cleartext document to create the encrypted document, wherein the document key is not accessible by the system; and

transmitting the encrypted document to the client device.