Claims

1. A system for storing private and public data on a cloud storage comprising:

a processing system unit having a processor and a memory communicatively connected to said processor, said memory having instructions executed by said processor to:

receiving a raw data;

extracting textual information;

categorising extracted textual information into public data and private data based on a policy file;

generating a hash value data for said private data, said generating said hash value data for said private data comprises:

determining number of k-consecutive text to be generated;

generating a hash value for each of a plurality of texts in said private data;

generating a subsequent hash value for each of k-consecutive text in said private data;

generating said hash value data by appending said hash value for each of said plurality of texts in said private data and said subsequent hash value for each of k-consecutive text in said private data to said hash value data, wherein k is less than the total number of text in said private data;

encrypting said raw data;

generating a package data including said encrypted raw data, said public data and said hash value data; and

storing said package data to said cloud storage.

2. The system according to claim 1, wherein said instructions to categorising extracted textual information into public data and private data based on said policy file comprises instructions to:

retrieving said policy file from said memory;

comparing said extracted textual information with a plurality of texts in said policy file; and

categorising said extracted textual information in said private data in response to said extracted textual information matches one of said plurality of texts in said policy file.

3. The system according to claim 2, wherein said instructions to categorising extracted textual information into public data and private data based on said policy file comprises instructions to:

categorising said extracted textual information in said public data in response to said extracted textual information that does not match any one of said plurality of texts in said policy file.

4. The system according to claim 1, wherein said instructions to extracting textual information comprises instructions to:

reading said raw data;

determining portion in said raw data that contains textual information;

generating said extracted textual information with said portion of said raw data being determined to be textual information.

~~5. The system according to claim 1, wherein said instructions to generating said hash value data for said private data comprises instructions to:~~

~~generating a hash value for each of a plurality of texts in said private data; and~~

~~generating said hash value data by appending said hash value for each of said plurality of texts in said private data to said hash value data.~~

~~6. The system according to claim 1, wherein said instructions to generating said hash value data for said private data comprises instructions to:~~

~~determining number of k-consecutive text to be generated;~~

~~generating a hash value for each of a plurality of texts in said private data;~~

~~generating a subsequent hash value for each of k-consecutive text in said private data;~~

~~generating said hash value data by appending said hash value for each of said plurality of texts in said private data and said subsequent hash value for each of k-consecutive text in said private data to said hash value data, wherein k is less than the total number of text in said private data.~~

~~57~~. The system according to claim ~~16~~, wherein k is equal to said total number of text in said private data.

~~68~~. The system according to claim ~~16~~, wherein k is predetermined and can be retrieved from said policy file.

~~79~~. The system according to claim 1, wherein said memory further comprises instructions to:

reading a query text string received;

categorising said query text string into said public data and said private data based on said policy file;

generating a hash value data for said private data;

generating a query string based on said hash value data for said private data and said public data;

transmitting said query string to said cloud storage.

~~810~~. The system according to claim ~~79~~, wherein said cloud storage comprises:

a processor and a memory communicatively connected to said processor, said memory having instructions executed by said processor to:

determining the type of query string;

retrieving an encrypted raw data associated with said query string in response to determining said type of query string is a request for encrypted raw data; and

transmitting said encrypted raw data to said processing system.

~~911~~. The system according to claim ~~79~~, wherein said cloud storage comprises:

a processor and a memory communicatively connected to said processor, said memory having instructions executed by said processor to:

determining the type of query string;

retrieving public data associated to said query string in response to determining said type of query string is a request for public data; and

transmitting said public data to said processing system.

102. The system according to claim 911, wherein said instructions to retrieving public data associated with said query string comprises instructions to:

reading said query string;

performing matching of text in said query string with text in package data stored in said memory in said cloud storage; and

retrieving every package data that includes text that matches said text in said query string;

extracting public data from each of said package data; and

ranking each of said public data according to number of texts that match said package data associated to said public data.

113. The system according to claim 1 further comprising:

a device for providing said raw data, wherein said processing unit is communicatively connected to said device to receive said raw data.

124. The system according to claim 113 wherein said device is a wearable medical device for tracking personal health status.

135. A method for storing private and public data on a cloud storage comprising:

receiving a raw data;

extracting textual information;

categorising extracted textual information into public data and private data based on a policy file;

generating a hash value data for said private data, said generating said hash value data for said private data comprises:

determining number of k-consecutive text to be generated;

generating a hash value for each of a plurality of texts in said private data;

generating a subsequent hash value for each of k-consecutive text in said private data;

generating said hash value data by appending said hash value for each of said plurality of texts in said private data and said subsequent hash value for each of k-consecutive text in said private data to said hash value data, wherein k is less than the total number of text in said private data;

encrypting said raw data;

generating a package including said encrypted raw data, said public data and said hash value data; and

storing said package to said cloud storage.

146. The method according to claim 135, wherein said step of categorising extracted textual information into public data and private data based on said policy file comprises:

retrieving said policy file from said memory;

comparing said extracted textual information with a plurality of texts in said policy file; and

categorising said extracted textual information in said private data in response to said extracted textual information matches one of said plurality of texts in said policy file.

157. The method according to claim 146, wherein said step of categorising extracted textual information into public data and private data based on said policy file comprises:

categorising said extracted textual information in said public data in response to said extracted textual information that does not match any one of said plurality of texts in said policy file.

168. The method according to claim 135, wherein said step of extracting textual information comprises:

reading said raw data;

determining portion in said raw data that contains textual information;

generating said extracted textual information with said portion of said raw data being determined to be textual information.

~~19. The method according to claim 15, wherein said step of generating said hash value data for said private data comprises:~~

~~generating a hash value for each of a plurality of texts in said private data; and~~

~~generating said hash value data by appending said hash value for each of said plurality of texts in said private data to said hash value data.~~

~~20. The method according to claim 15, wherein said step of generating said hash value data for said private data comprises:~~

~~determining number of k-consecutive text to be generated;~~

~~generating a hash value for each of a plurality of texts in said private data;~~

~~generating a subsequent hash value for each of k-consecutive text in said private data;~~

~~generating said hash value data by appending said hash value for each of said plurality of texts in said private data and said subsequent hash value for each of k-consecutive text in said private data to said hash value data, wherein k is less than the total number of text in said private data.~~

1721. The method according to claim 1320, wherein k is equal to said total number of text in said private data.

1822. The method according to claim 1320, wherein k is predetermined and can be retrieved from said policy file.

1923. The method according to claim 135, further comprising:

reading a query text string received;

categorising said query text string into said public data and said private data based on said policy file;

generating a hash value data for said private data;

generating a query string based on said hash value data for said private data and said public data;

transmitting said query string to said cloud storage.

204. The method according to claim 1923, wherein said cloud storage upon receiving said query string performs the following steps:

determining the type of query string;

retrieving an encrypted raw data associated with said query string in response to determining said type of query string is a request for encrypted raw data; and

transmitting said encrypted raw data to said processing system.

215. The method according to claim 1923, wherein said cloud storage upon receiving said query string performs the following steps:

determining the type of query string;

retrieving public data associated to said query string in response to determining said type of query string is a request for public data; and

transmitting said public data to said processing system.

226. The method according to claim 215, wherein said step of retrieving public data associated with said query string comprises:

reading said query string;

performing matching of text in said query string with text in package data stored in said memory in said cloud storage; and

retrieving every package data that includes text that matches said text in said query string;

extracting public data from each of said package data; and

ranking each of said public data according to number of texts that match said package data associated to said public data.