(12)Indian Patent Application

(21) Application Number: 201741006088

(22) Filing Date: 21/02/2017 (43) Publication Date: 24/08/2018

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): SARAVANAKUMAR, TS

(51) International Classifications: H04L 9/08

(54) Title: A METHOD AND SYSTEM FOR PROVIDING DATA SECURITY

(57) Abstract: The invention relates to a method and system for encrypting a plurality of datasets for providing data security. Each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset The disclosed system and method generates a first key by randomly choosing one or more of the plurality of data from the dataset and the selected one or more data is other than the first data in the dataset. The disclosed method and system generates a second key using a combination of first key and the first data of the dataset. The dataset is encrypted using the second key.

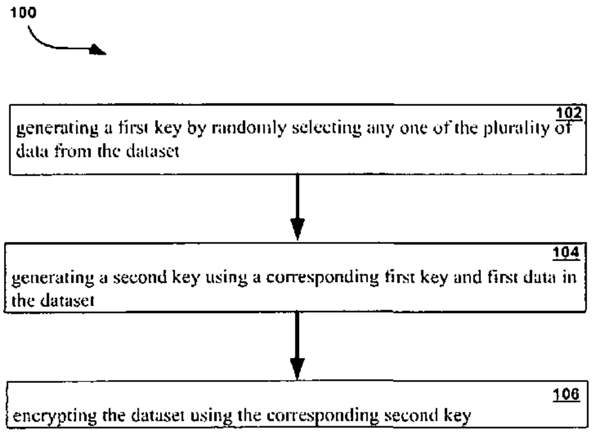
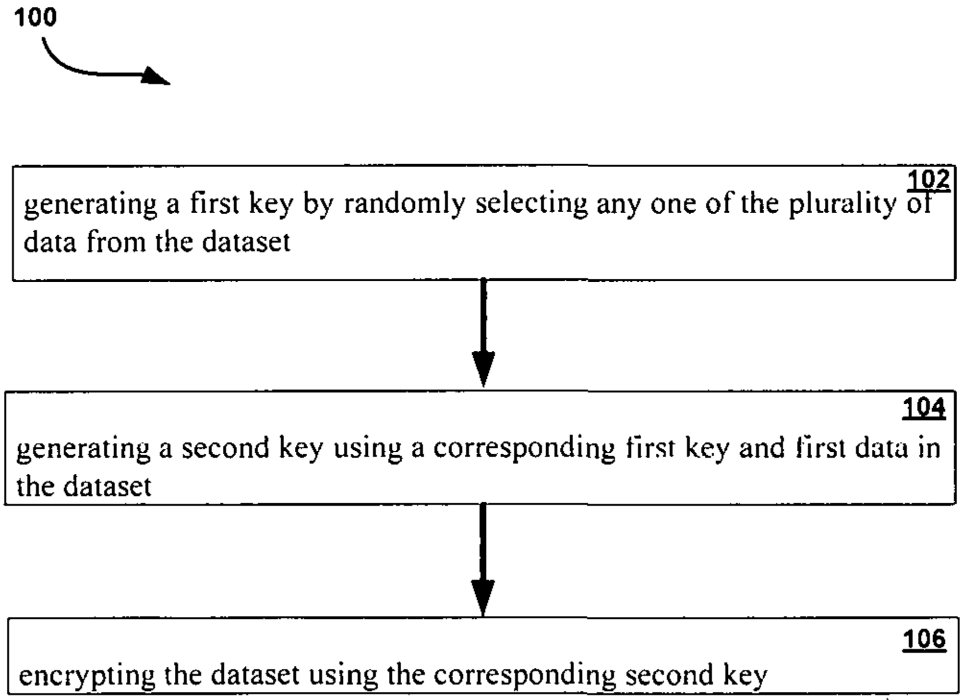

100
102
generating a first key by randomly selecting any one of the plurality of data from the dataset
104
generating a second key using a corresponding first key and first data in the dataset
106
encrypting the dataset using the corresponding second key

Figure 1

ABSTRACT

A METHOD AND SYSTEM FOR PROVIDING DATA SECURITY

The invention relates to a method and system for encrypting a plurality of datasets for providing data security. Each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset The disclosed system and method generates a first key by randomly choosing one or more of the plurality of data from the dataset and the selected one or more data is other than the first data in the dataset. The disclosed method and system generates a second key using a combination of first key and the first data of the dataset. The dataset is encrypted using the second key.


100
102
generating a first key by randomly selecting any one of the plurality of data from the dataset
104
generating a second key using a corresponding first key and first data in the dataset
106
encrypting the dataset using the corresponding second key

We Claim:

1. A method of encrypting one or more datasets of a plurality of datasets, wherein each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset, the method comprising:

dynamically generating a first key by randomly selecting one or more of the plurality of data from the dataset, the selected one or more data being other than a corresponding first data;

generating a second key using a combination of the corresponding first key and the first data of the dataset; and

encrypting the dataset using the corresponding second key.

2. The method as claimed in claim1 wherein the encrypting the data of the dataset using the corresponding second key includes excluding encrypting the first data.

3. The method as claimed in claim1, wherein the first data corresponds to a public key and the first key corresponds to a private key of the asymmetric public-private key pair.

4. The method as claimed in claim 1, wherein the randomly selecting any one of the plurality of data uses a random number generator.

5. The method as claimed in claim 1 wherein the random number is generated using current system timestamp.

6. A system for providing data security for one or more datasets of a plurality of datasets wherein each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset, the system comprising:

a key generating module configured to generate a key;

an encryption module configured to encrypt the dataset using the key; and

a decryption module configured to decrypt the encrypted dataset using the key.

Dated this 21st day of February 2017

Mohammed Faisal (INPA No: 1941)
Head, IPR Dept.
L&T Technology Services Limited
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai, TN, 600089

FIELD OF INVENTION

The invention generally relates to system and methods for providing data security and more particularly to generating a digital key for encrypting datasets.

BACKGROUND

Information security is very crucial in today's world. The information is stored in various places like cloud, mails and remote storage areas. The stored information is confidential and should not be read by anyone.

Certain known public key/private key cryptosystems typically utilize the random number approach in key generation. However, it is believed that additional security aspects for public key/private key generation can be obtained by utilizing measures other than strictly using a random number in the key generation algorithms.

Conventionally, when a target file is encrypted, it is normal that the entire target file is encrypted using a fixed encryption key generated by, for example, a password, etc. However, since an encrypting process has been performed using a fixed encryption key according to the conventional system, the security level of each data item is averaged. In addition, when there are a plurality of items containing the same data, the same encryption results are output, thereby causing the possibility that the encryption key can be decrypted.

Accordingly, there is a need for improved methods for generating cryptographic keys that aid in more data security, especially in asymmetric public key/private key cryptosystems.

Hence, there is a need for a method of encrypting datasets that provide protection of data from the power of the system administrator or DBA or file owner.

The present invention is directed to overcoming one or more of the problems as set forth above.

SUMMARY OF THE INVENTION

Exemplary embodiments of the invention disclose a method and system for encrypting one or more datasets of a plurality of datasets, wherein each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset. According to an exemplary embodiment, the disclosed method and system dynamically generates a first key by randomly selecting one or more of the plurality of data from the dataset and the selected data being other than a corresponding first data. A second key is generated using a combination of the corresponding first key and the first data of the dataset. The dataset is encrypted using the corresponding second key.

BRIEF DESCRIPTION OF DRAWINGS

Other objects, features, and advantages of the invention will be apparent from the following description when read with reference to the accompanying drawings. In the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

Figure 1 illustrates a block diagram of a process for dynamically generating a digital key for encrypting a dataset, according to an exemplary embodiment of the invention; and

Figure 2 illustrates an exemplary system for providing data security, according to one embodiment of the invention.

DETAILED DESCRIPTION OF DRAWINGS

The following description with reference to the accompanying drawings is provided to assist in a comprehensive understanding of exemplary embodiments of the invention as defined by the claims and their equivalents. It includes various specific details to assist in that understanding but these are to be regarded as merely exemplary. Accordingly, those of ordinary skill in the art will recognize that various changes and modifications of the embodiments described herein can be made without departing from the scope and spirit of the invention. In addition, descriptions of well-known functions and constructions are omitted for clarity and conciseness.

According to embodiments of the invention, a system and method for providing data security is disclosed.

FIG. 1 illustrates a block diagram of the process 100 for encrypting one or more datasets of the plurality of datasets, wherein each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset, according to an embodiment of the invention. According to an embodiment, the first data may be in plain text. According to an exemplary embodiment, the dataset may be a set of records in a database. According to another exemplary embodiment, the dataset may be a table in a Microsoft word, excel or access document. According to yet another embodiment, the dataset may be a portion of the table in the document. According to an embodiment, the datasets may be stored at client side or server side.

At step 102, a first key is generated dynamically. According to an embodiment, the first key may be generated by randomly selecting one or more of the plurality of data from the dataset and the selected data may be other than the first data in the dataset. According to an exemplary embodiment, the dataset may correspond to a column data in a database and the first data may correspond to a primary key in the database. According to another exemplary embodiment, the dataset may correspond to a row data in a database. According to yet another exemplary embodiment, the dataset may correspond to a list of data.

According to another embodiment, the randomly selecting any one of the plurality of data from the dataset is based on an input index stored in a configuration file. According to yet another embodiment, the configuration file may be stored at client or server. According to another embodiment, the randomly selecting any one of the plurality of data uses a random number generator. The random number generator may generate random number using current system timestamp. According to another embodiment, the random number may be generated by a pseudo random number generator.

At step 104, a second key is generated by combining the corresponding first key and first data in the dataset. According to an embodiment, the first data corresponds to a public key and the first key corresponds to a private key of the asymmetric public-private key pair. According to another embodiment, the second key may be valid only for a pre-defined time period. After the period of time expires, a new second key may be generated. According to another embodiment, the pre-defined time period may be mentioned in a configuration file.

At step 106, the dataset is encrypted using the corresponding second key. According to an embodiment, all data in the dataset except the first data may be encrypted with the second key. According to another embodiment, selected data in the dataset may be encrypted with the second key.

FIG. 2 illustrates an exemplary system 200 for providing data security for one or more datasets of a plurality of datasets wherein each of the plurality of datasets has an asymmetric key pair for cryptographic encryption and decryption and one data in each dataset is a first data that uniquely identifies the dataset, according to one embodiment of the present invention.

The disclosed system 200 may include a subsystem 202 having a key generation module 204, an encryption module 208 and a decryption module 210.

The key generation module 204 may include a processing module 206. The processing module 206 may generate a first key dynamically by randomly selecting one or more of the plurality of data from the dataset and the selected data may be other than a corresponding first data. Further, the processing module 206 may generate a second key using a combination of the corresponding first key and the first data of the dataset. According to an embodiment, the second key may be generated at a client side or at server side.

The encryption module 208 may encrypt the selected dataset using the corresponding second key. According to an embodiment, the selection of the dataset for encryption may be automated. According to another embodiment, the selection of the dataset for encryption may be done manually by a user. According to yet another embodiment, the generated second key may be valid only for a predetermined period. A new second key may be generated after expiry of a predetermined time period. According to a further embodiment, the encryption module 208 may encrypt the entire dataset except the first data. According to another embodiment, the encryption module 208 may encrypt selected data in the dataset.

According to an embodiment, the processor 206 may be in communication with a network module 212. According to another embodiment, the second key may be transferred to another subsystem 214. The subsystem 214 may be a client or a server. According to another embodiment, the network module may include a communication network. According to an embodiment, the communication network may be a wired or wireless communication network. The wireless communication network may be such as, but not limited to, Zigbee, Lora, Wi-Fi and Bluetooth.

The decryption module 210 may decrypt the encrypted dataset using the corresponding second key. The decryption process may result in one or more data of the dataset that is randomly selected for encrypting the data of the dataset. Using the decrypted one or more data and the first data of the dataset, the other data of the dataset may be decrypted.

According to an embodiment, a user trying to decrypt the dataset may need decrypt permission from owner of the dataset. The decrypt permission may be given to the user only on successful authentication of the user.

According to another embodiment, the encryption and decryption process may be automated.

In the drawings and specification there has been set forth preferred embodiments of the invention, and although specific terms are employed, these are used in a generic and descriptive sense only and not for purposes of limitation. Changes in the form and the proportion of parts, as well as in the substitution of equivalents, are contemplated as circumstances may suggest or render expedient without departing from the spirit or scope of the invention.

Throughout the various contexts described in this disclosure, the embodiments of the invention further encompass computer apparatus, computing systems and machine-readable media configured to carry out the foregoing systems and methods. In addition to an embodiment consisting of specifically designed integrated circuits or other electronics, the present invention may be conveniently implemented using a conventional general purpose or a specialized digital computer or microprocessor programmed according to the teachings of the present disclosure, as will be apparent to those skilled in the computer art.

Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art. The invention may also be implemented by the preparation of application specific integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be readily apparent to those skilled in the art.

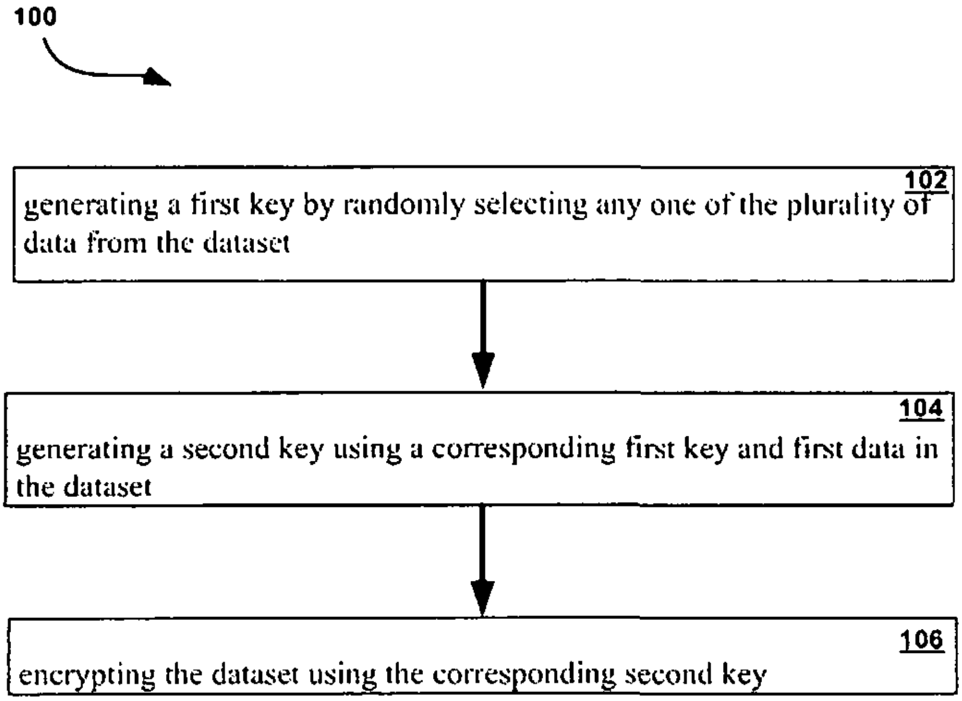

100
102
generating a first key by randomly selecting any one of the plurality of data from the dataset
104
generating a second key using a corresponding first key and first data in the dataset
106
encrypting the dataset using the corresponding second key

Figure 1

Mohammed Faisal (INPA No: 1941)
Head, IPR Dept.
L&T Technology Services Limited
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai – 600089

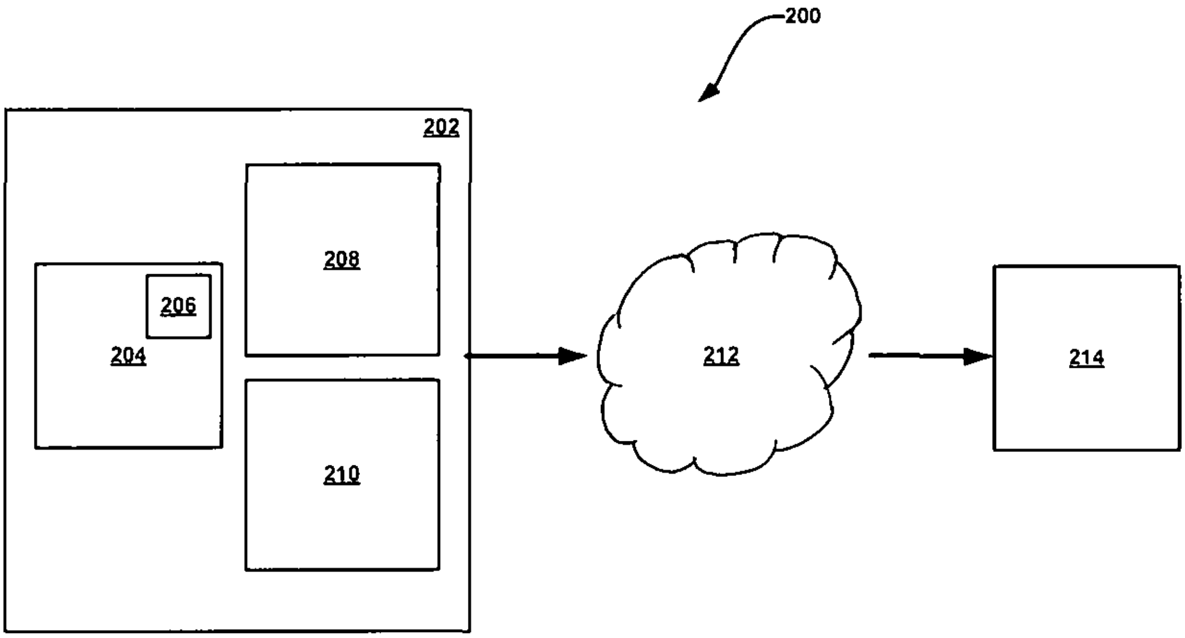


Figure 2

Mohammed Faisal (INPA No: 1941)
Head, IPR Dept.
L&T Technology Services Limited
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai – 600089