(12)Indian Patent Application

---

(21) Application Number: 201641043251

(22) Filing Date: 19/12/2016 (43) Publication Date: 22/06/2018

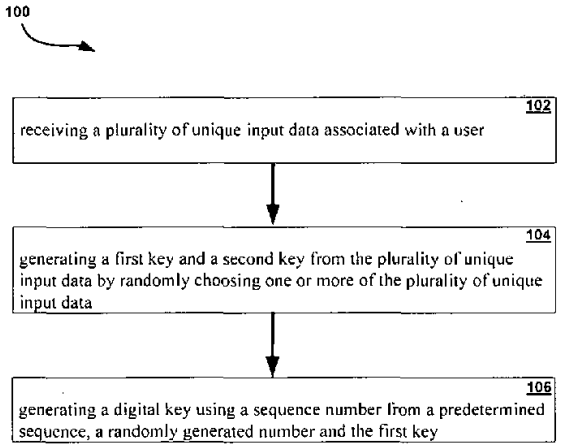
(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): PRIYANKA, S.
NAGAJEYA, RAMALINGAM M.

(51) International Classifications: G06K 9/00 H04L 9/08

(54) Title: A METHOD AND SYSTEM FOR DIGITAL KEY GENERATION FROM USER DATA

(57) Abstract: The invention relates to a method and system for generating a digital key for providing a secure access of an application to a user. The disclosed system and method receives a plurality of unique input data associated with the user, generates a first key and a second key from the plurality of unique input data by randomly choosing one or more of the plurality of unique input data and generates a digital key using a sequence number, a randomly generated number and the first key. The disclosed method and system validates the digital key and provides access of the application to the user based on a result of validation.



## FIELD OF INVENTION

The invention generally relates to system and methods for providing a secure access to internet applications and more particularly to generating and verifying a digital key to provide secure access to the internet applications.

## BACKGROUND

Safeguarding of cryptographic keys is especially important in connection with the conduct of electronic transactions such as, for example, financial transactions. Facilitating the adoption and use of cryptography in such electronic communications is important, as demand for greater security, reliability, and accountability in the electronic communications is believed to be increasing.

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 during in the key generation algorithms.

Apart from random number approach in key generation, there are other existing algorithms such as time based one-time password (OTP) generation algorithms, Advanced Encryption Standard (AES) algorithm, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) algorithm and hashing algorithm. However, the existing approaches suffer from their own drawbacks. For example, in time based OTP generation algorithm, the same secret key is shared by client and server and timer should be in synchronization. In dynamic password generation using AES

algorithm, the same digital key seed and serial number is used at client and server side and digital key generator may calculate a same dynamic digital key change over time using a high intensity symmetric encryption algorithm based on the current time. In RSA algorithm, public and private key is generated using prime numbers and public key along with message is passed to server. The drawback with RSA is while decoding message, private key should be known at server and it uses prime numbers. Its output will be always same for the same input. Hashing is a method to map data of arbitrary length to fixed length. Hashing is used in many cryptographic algorithms for mapping of data, for example in hash message authentication code (HMAC), key is passed with hashed data and during validation key should be known.

Accordingly, there is a need for improved methods for securely generating and protecting cryptographic keys, especially in asymmetric public key/private key cryptosystems.

Hence, there is a need for a method of encrypting user data that uses a combination of user data, random number and sequence number to generate dynamic key, thereby tracking source impossible.

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 generating a digital key for providing a secure access of an application to a user. According to an exemplary embodiment, the disclosed method and system receives a plurality of unique input data associated with the user. A first key and a second key is generated from the unique input data

by randomly choosing one or more of the plurality of unique input data. A digital key is generated using a sequence number from a predetermined sequence, a randomly generated number and the first key.

According to an exemplary embodiment, the disclosed method and system validates the digital key and provides access of the application to the user based on a result of validation.

## 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 generating a digital key for providing a secure access of an application to a user, according to an exemplary embodiment of the invention; and

Figure 2 illustrates an exemplary system for providing a secure access of an application to a user, 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 generating a digital key for providing a secure access of an application to a user is disclosed.

FIG. 1 illustrates a block diagram of the process 100 for generating a digital key for providing a secure access of an application to a user according to an embodiment of the invention.

At step 102, a plurality of unique input data associated with a user is received. According to an embodiment, the unique input data associated with the user may be such as, but not limited to, a phone number, date of birth, PAN number, aadhaar card number, account number, election ID card number and driving license number. According to an embodiment, any other user parameter may be used to generate the digital key. According to another embodiment, the number of unique user data may be in a range from 1 to 20. According to another embodiment, the unique input data may be received through a user interface. According to yet another embodiment, the user interface may be a graphical user interface. According to another embodiment, the unique input data may be generated by a system.

At step 104, a first key and a second key is generated from the plurality of unique input data by randomly choosing one or more of the plurality of unique input data. The first key and the second key may be generated using any of the known encryption algorithms. According to an embodiment, the first key may be a public key and the second key may be a private key of a

public-private key pair. According to another embodiment, the randomly choosing one or more of the plurality of unique input data is based on an input index stored in a configuration file. According to yet another embodiment, the input index may be stored in a server. According to yet another embodiment, the input index may be used to determine the one or more unique data from a plurality of unique input data that is used to generate public key and private key. According to an embodiment, the public key may be used in the generation of digital key and the private key may be kept as secret. The tracking back to the input data from the generated digital key may be impossible without knowing the private key.

At step 106, a digital key is generated using a sequence number from a predetermined sequence, a randomly generated number and the first key. According to an embodiment, the digital key may be a unique and random alphanumeric data. According to another embodiment, the digital key may be alphanumeric data of 6 or 8 or fixed number of characters. According to an embodiment, the first key may be a public key of a public-private key pair. According to another embodiment, the random number is generated using current system timestamp. According to another embodiment, the random number may be generated by a random number generator or pseudo random number generator. According to an embodiment, the sequence number is determined from a predefined sequence. According to another embodiment, the predefined sequence may be in a range from 1 to 15. According to an embodiment, the generated digital key may be used to validate a user of an application. According to another embodiment, the digital key may be valid only for a predetermined period. After the period of time expires, a new digital key may be generated. According to an embodiment, the digital key may be valid only for a time period as mentioned in a configuration file.

According to an embodiment, the user may have to enter digital key along with username and password to access the application.

FIG. 2 illustrates an exemplary system 200 for providing a secure access of an application to a user, according to one embodiment of the present invention.

The disclosed system 200 may include a client component 202, a communication network 208 and a server component 210.

The client component may include an input module 204 and a processing module 206.

The input module 204 may receive a plurality of unique input data associated with a user. According to an embodiment, the unique input data associated with the user may be such as, but not limited to, a phone number, date of birth, PAN number, aadhaar card number, account number, election ID card number and driving license number. According to another embodiment, the number of unique user data may be in a range from 1 to 20. According to another embodiment, the unique input data may be received through a user interface. According to yet another embodiment, the user interface may be a graphical user interface. According to another embodiment, the unique input data may be generated by a system.

The processing module 204 may generate a public key and a private key from the unique input data by randomly choosing any one of the plurality of unique input data. According to an embodiment, the first key may be a public key and the second key may be a private key of a public-private key pair. According to another embodiment, the randomly choosing one or more of the plurality of unique input data is based on an input index stored in a configuration file.

According to yet another embodiment, the input index may be used to determine the one or more unique data from a plurality of unique input data that is used to generate public key and private key.

The processing module 204 may further generate a digital key using a sequence number from a predetermined sequence, a randomly generated number and the public key. According to an embodiment, the first key may be a public key of a public-private key pair. According to another embodiment, the random number is generated using current system timestamp. According to yet another embodiment, the random number may be generated by a random number generator or pseudo random number generator. According to an embodiment, the sequence number is determined from a predefined sequence. According to another embodiment, the predefined sequence may be in a range from 1 to 15. According to yet another embodiment, the generated digital key may be used to validate a user of an application. The digital key may be valid only for a predetermined period. A new digital key may be generated after expiry of the predetermined period.

According to an embodiment, the processor 204 may be in communication with a network module 208. The digital key may be transferred from the client component 202 to the server component 210 through the network module 208. 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 server component 210 may receive the transmitted digital key from the client component 202. According to an embodiment, the server component 210 may include a validation module.

The validation module may decode the digital key received by the server component 210. According to an embodiment, the validation module may decode the public key and sequence number from the digital key entered by user.

The validation module compares the public key decoded from the digital key with a public key generated from unique input data stored in the server component 210 and comparing a sequence number decoded from the digital key with a stored sequence number. In other words, the decoded sequence number may be validated with stored sequence number. According to an embodiment, the sequence number may be stored in a configuration file or in a server. According to another embodiment, the sequence number validation may ensure that previously generated digital keys entered by the user may be rendered invalid.

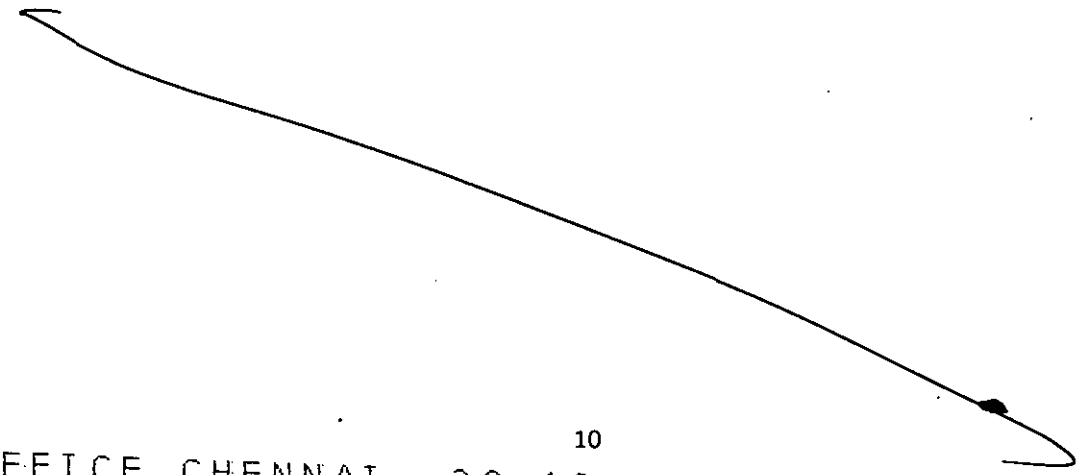
According to yet another embodiment, the validation module may provide access of the application to the user based on a result of validation. The providing access of the application to the user based on a result of validation includes providing access of the application on successful validation of the digital key and denying access of the application on unsuccessful validation of the digital key.

The encryption algorithm disclosed in the specification does not use existing technologies such as time based OTP generation algorithms, AES algorithm, RSA algorithm and hashing algorithm for encryption. The invention is safe from different type of hackers attack like brute force, dictionary and key logger attacks. The invention uses a unique encoding and decoding logic and makes prediction of next digital key pattern impossible. The encryption uses part of user data to generate the dynamic key thereby tracking back to source is impossible. The dynamic digital key generated using the disclosed invention is secure and strong.

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.



We Claim:

1. A method of generating a digital key for providing a secure access of an application to a user, the method comprising:

receiving a plurality of unique input data associated with the user;

generating a first key and a second key from the plurality of unique input data by randomly choosing one or more of the plurality of unique input data; and

generating a digital key using a sequence number from a predetermined sequence, a randomly generated number and the first key.

2. The method as claimed in claim 1 wherein the unique input data associated with a user is one of a phone number, date of birth, PAN number, aadhaar card number, account number, election ID card number and driving license number.

3. The method as claimed in claim 1 wherein the input data is generated by a system.

4. The method as claimed in claim 1 wherein the randomly choosing one or more of the plurality of unique input data is based on an input index stored in a configuration file.

5. The method as claimed in claim 1 wherein the first key is a public key and the second key is a private key of a public-private key pair.

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

7. A system for providing a secure access of an application to a user, the system comprising:

a client component configured to generate a digital key, the client component including:

an input module configured to receive a plurality of unique input data associated with a user;

a processing module configured to:

generate a public key and a private key from the unique input data by randomly choosing any one of the plurality of unique input data; and

generate a digital key using a sequence number from a predetermined sequence, a randomly generated number and the public key; and

a server component configured to receive the digital key transmitted from the client component and validate the digital key.

8. The system as claimed in claim 7, wherein the server component includes a validation module configured to:

decode the digital key received by the server component;

validate the digital key; and

provide access of the application to the user based on a result of validation.

9. The system as claimed in claim 8, wherein validating the digital key includes comparing a public key decoded from the digital key with a public key generated from unique input data stored in the server component and comparing a sequence number decoded from the digital key with a sequence number stored in a configuration file.

10. The system as claimed in claim 8, wherein the providing access of the application to the user based on a result of validation includes providing access of the application on successful validation of the digital key and denying access of the application on unsuccessful validation of the digital key.

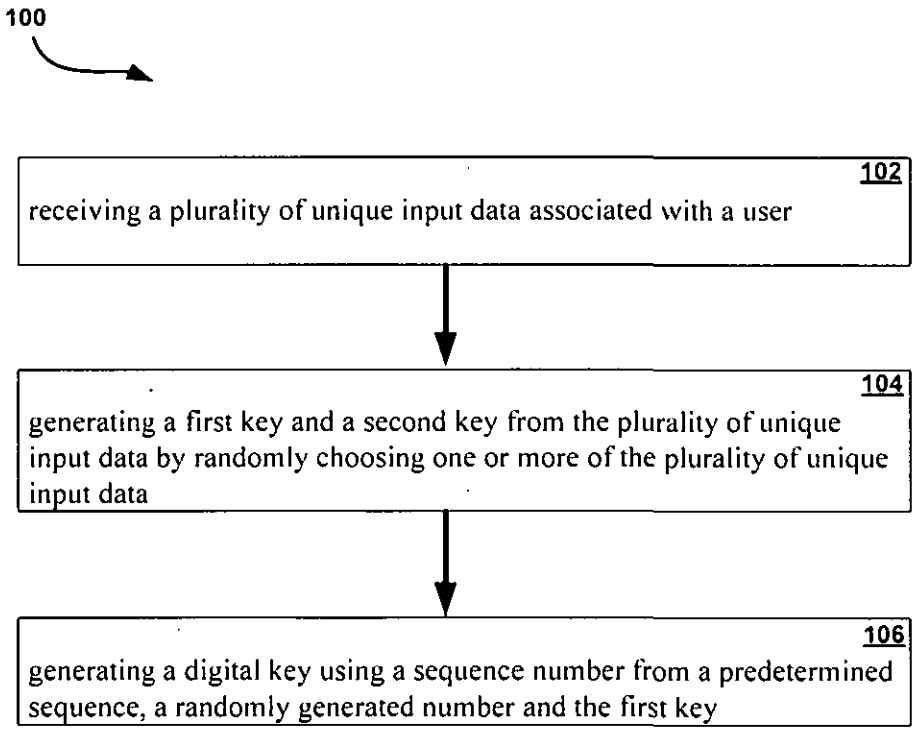
Dated this 19th day of December 2016

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

## ABSTRACT

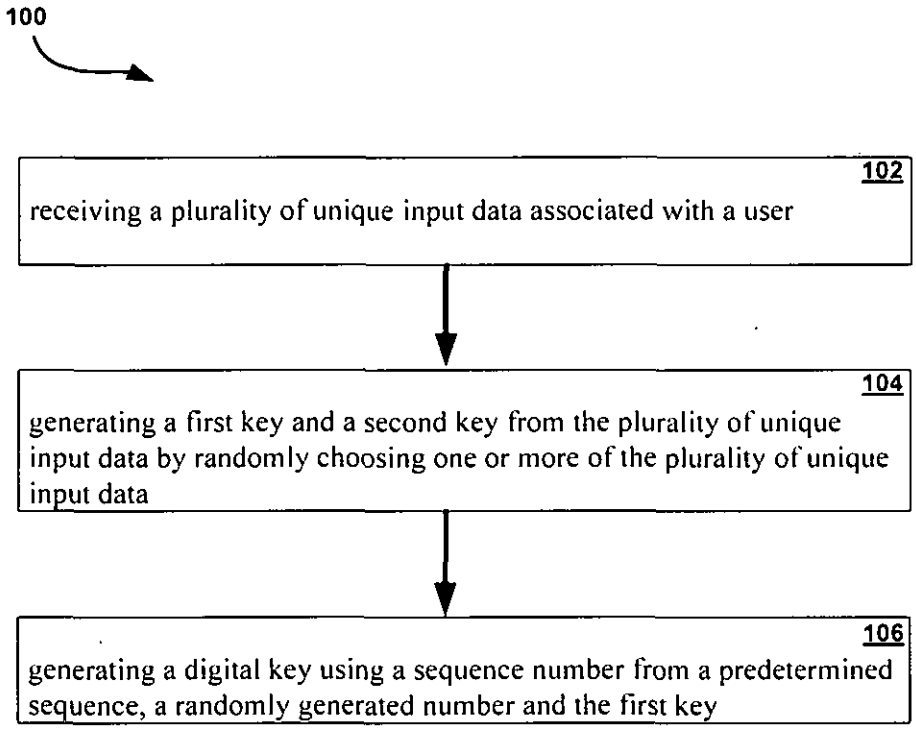
A METHOD AND SYSTEM FOR DIGITAL KEY GENERATION FROM USER DATA

The invention relates to a method and system for generating a digital key for providing a secure access of an application to a user. The disclosed system and method receives a plurality of unique input data associated with the user, generates a first key and a second key from the plurality of unique input data by randomly choosing one or more of the plurality of unique input data and generates a digital key using a sequence number, a randomly generated number and the first key. The disclosed method and system validates the digital key and provides access of the application to the user based on a result of validation.



L&T Technology Services Limited

Total number of Sheets: 2
Sheet No. 1 of 2




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

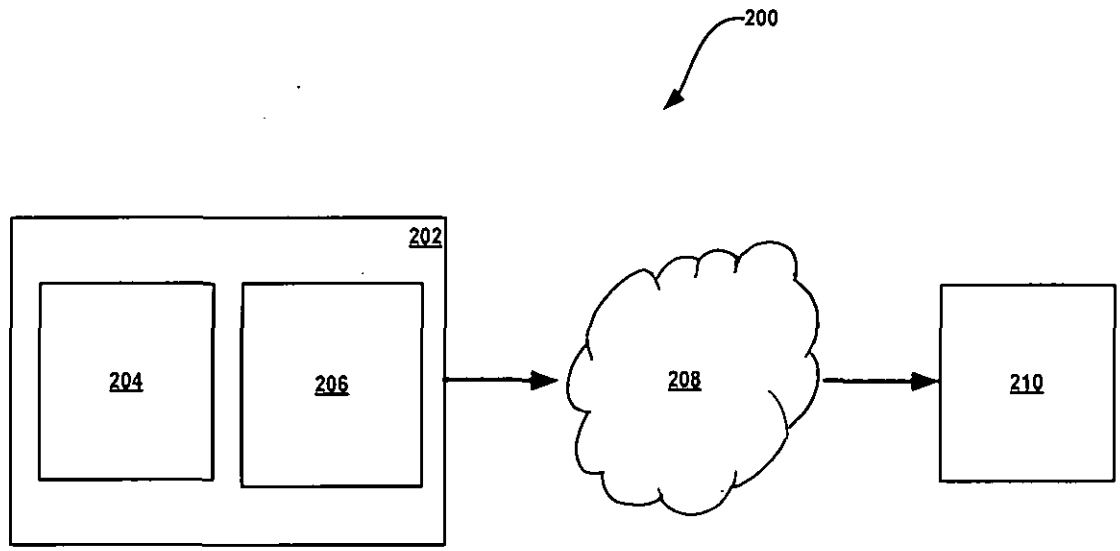



Figure 2

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