SYSTEM AND METHOD FOR AUTHORIZING A TRANSACTION

FIELD OF INVENTION

The invention relates to a system and a method for authorizing a transaction.

BACKGROUND

Currently, users typically provide a non-confidential user identifier (e.g. a user ID) and a confidential personal identification number (PIN) to gain access to a system. In this way, the PIN is used to authenticate the user to the system. Upon receiving the user ID and PIN, the system retrieves a registered PIN (that is stored in the system) based on the user ID and compares the registered PIN with the received PIN. The user is granted access only if the received PIN matches the registered PIN number. PINs are commonly used for automated teller machines (ATMs) and at points of sale (POS) for debit cards and credit cards. However, this method of authentication requires that the user remembers his PIN. If the user forgets his PIN, he would not be able to complete the transaction. He would need to seek the system administrator's assistance to retrieve his PIN or reset his PIN.

A need therefore exists to provide a system and a method for authorizing a transaction that seeks to address at least the above-mentioned problems.

SUMMARY

According to an aspect, the present disclosure refers to a system for authorizing a transaction, comprising: a biometric scanner obtaining biometric information from a user by detecting at least one of a physical feature and a behavioral feature of the user; an input device receiving account data relating to an account of the user; a controller (i) receiving the obtained biometric information from the biometric scanner, (ii) producing encrypted biometric information by encrypting the obtained biometric information, and (iii) generating a transaction code by converting the encrypted biometric information into alphanumeric, numeric or binary codes, and (iv) receiving, from the input device the account data relating to the

account of the user; a server receiving, from the controller, the account data and the transaction code; and a database, in communication with the server, storing the account data and a registration code associated with the account data, wherein in an enrollment phase, prior to the transaction, the controller derives the registration code, at least in part, using pre-registered biometric information of the user; wherein, the server, using the account received from the controller and inputted by the user during the transaction, (i) searches through a plurality of registered accounts stored in the database, (ii) identifies the registration code stored, in the database, in association with the account data received from the controller, said registration code having been previously derived by the controller, at least in part, using pre-registered biometric information of the user, (iii) performs a comparison of the identified registration code with the transaction code, and (iv) authorizes or denies the transaction on a basis of said comparison.

According to an example, there is provided a system for authorizing a transaction, comprising: a biometric scanner configured to obtain biometric information from a user; a controller configured to receive the obtained biometric information from the biometric scanner and to generate a transaction code based on the obtained biometric information, the controller being further configured to receive account data relating to an account of the user; a server configured to receive the account data and the transaction code from the controller; a database in communication with the server and having stored thereon the account data in association with a registered code, the registered code having been generated based on pre-obtained biometric information of the user; and wherein the server is operable to use the account data to identify the registered code and to authorize the transaction based on a comparison of the registered code with the transaction code.

In an example, the server may be operable to authorize the transaction if the transaction code corresponds with or matches the registered code; and the server may be operable to decline the transaction if the transaction code does not correspond with or match the registered code.

In an example, the system may further comprise a first encryptor in communication with the controller, the first encryptor configured to encrypt the obtained biometric information such that the controller generates the transaction code based on the encrypted biometric information. The system may further comprise a second encryptor in communication with the controller, the second

encryptor configured to encrypt the generated transaction code such that the controller sends the encrypted transaction code to the server.

In an example, the biometric scanner may comprise a fingerprint scanner configured to generate a digital representation based on a fingerprint of the user, and the biometric information may comprise the digital representation.

In an example, the biometric scanner may comprise an image capturing device configured to generate a digital representation based on an iris or retina of the user, and the biometric information may comprise the digital representation.

In an example, the account data may comprise one or more of: an account number, a credit card number, a user's name.

In an example, the database may store the account data in association with user information and the server may be further operable to provide the user information to the controller if the transaction is authorized.

In an example, the server may be further operable to permit funds to be taken from the account if the transaction is authorized.

In an example, the controller may be further configured to receive transaction data; and the server may be further configured to receive the transaction

data from the controller; and wherein the server may be operable to authorize the transaction based on the transaction data.

In an example, the transaction data may comprise a transaction amount and the database may store the account data in association with an amount of available funds in the account, wherein the server may be operable to use the account data to identify the amount of available funds in the account and to authorize the transaction only if the amount of available funds in the account is equal to or greater than the transaction amount.

In an example, the controller may be configured to generate the transaction code and registered code by converting the biometric information of the user into alphanumeric, numeric or binary codes.

According to an example, there is provided a method of authorizing a transaction, the method comprising: obtaining biometric information from a user; receiving account data relating to an account of the user; generating a transaction code based on the obtained biometric information; storing the account data in association with a registered code, the registered code having been generated based on pre-obtained biometric information of the user; using the account data to identify the registered code; and authorizing the transaction based on a comparison of the registered code with the transaction code.

In an example, authorizing may comprise authorizing the transaction if the transaction code corresponds with or matches the registered code. In an embodiment, authorizing may also comprise declining the transaction if the transaction code does not correspond with or match the registered code.

In an example, generating may comprise: encrypting the obtained biometric information; and generating the transaction code based on the encrypted biometric information.

In an example, the method may further comprise encrypting the generated transaction code.

In an example, the method may further comprise the step of permitting funds to be taken from the account if the transaction is authorized.

In an example, the method may further comprise receiving transaction data; and wherein authorizing the transaction is based on the transaction data.

In an example, storing may comprise storing the account data in association with an amount of available funds in the account, wherein using may comprise using the account data to identify the amount of available funds in the account, wherein the transaction data may comprise a transaction amount, and wherein authorizing may comprise authorizing the transaction only if the amount of available funds in the account is equal to or greater than the transaction amount.

In an example, the method may further comprise the step of generating the transaction code and registered code by converting the biometric information of the user into alphanumeric, numeric or binary codes.

BRIEF DESCRIPTION OF THE DRAWINGS

Example embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Fig. 1 is a schematic diagram of a system for authorizing a transaction, according to an embodiment of the invention;

Fig. 2 is a flow chart illustrating a method of authorizing a transaction, according to an embodiment of the invention;

Fig. 3 is a sequence diagram of a method of authorizing a transaction, according to an embodiment of the invention; and

Fig. 4 is a schematic of a computer system for implementing the system and method for authorizing a transaction in example embodiments of the invention.

CLAIMS

1. A system for authorizing a transaction, comprising:

a biometric scanner obtaining biometric information from a user by detecting at least one of a physical feature and a behavioral feature of the user;

an input device receiving account data relating to an account of the user;

a controller (i) receiving the obtained biometric information from the biometric scanner, (ii) producing encrypted biometric information by encrypting the obtained biometric information, and (iii) generating a transaction code by converting the encrypted biometric information into alphanumeric, numeric or binary codes, and (iv) receiving, from the input device the account data relating to the account of the user;

a server receiving, from the controller, the account data and the transaction code; and

a database, in communication with the server, storing the account data and a registration code associated with the account data, wherein in an enrollment phase, prior to the transaction, the controller derives the registration code, at least in part, using pre-registered biometric information of the user;

wherein, the server, usingthe account received from the controller and inputted by the user during the transaction,

(i) searches through a plurality of registered accounts stored in the database,

(ii) identifies the registration code stored, in the database, in association with the account data received from the controller, said registration code having been previously derived by the controller, at least in part, using pre-registered biometric information of the user,

(iii) performs a comparison of the identified registration code with the transaction code, and

(iv) authorizes or denies the transaction on a basis of said comparison.

2. The system of claim 1, wherein the server authorizes the transaction if the transaction code matches the registration code.

3. The system of claim 1, wherein the server declines the transaction if the transaction code does not match the registration code.

4. The system of claim 1, wherein the controller further encrypts the generated transaction code such that the controller sends the encrypted transaction code to the server.

5. The system of claim 1, wherein the biometric scanner comprises a fingerprint scanner, wherein the fingerprint scanner generates a digital representation based on a fingerprint of the user, and the biometric information comprises the digital representation.

6. The system of claim 1, wherein the biometric scanner comprises an image capturing device, wherein the image capturing device generates a digital representation based on an iris or retina of the user, and the biometric information comprises the digital representation.

7. The system of claim 1, wherein the account data comprises one or more of: an account number, a credit card number, a name of the user.

8. The system of claim 1, wherein the database stores the account data in association with user information, and the server provides the user information to the controller if the transaction is authorized.

9. The system of claim 1, wherein the server further permits funds to be taken from the account if the transaction is authorized.

10. The system of claim 1, wherein the controller further receives transaction data, and the server is further receives the transaction data from the controller; and

wherein the server authorizes the transaction based on the transaction data.

11. The system of claim 10, wherein the transaction data comprises a transaction amount and the database stores the account data in association with an amount of available funds in the account, wherein the server uses the account data to identify the amount of available funds in the account and to authorize the transaction only if the amount of available funds in the account is equal to or greater than the transaction amount.