

[0005] These and other deficiencies exist. Thus, it may be beneficial to provide exemplary systems, methods, and computer-accessible mediums which allow for verification of cards being used for transactions, to overcome at least some of the deficiencies described herein.

SUMMARY

[0006] Aspects of the disclosed technology include systems, methods, and computer-accessible mediums for user verification through the interaction of user's short-range transceiver, such as a contactless card, with a client device. User verification may be provided in the context of reading two types of data from the short-range transceiver, such as a contactless card, using a client device such that identifiers and other information may be obtained from each data type and compared with stored information, including stored user identifier data. Matching stored user identifier data to two forms of identification data obtained from a short-range transceiver, such as a contactless card, provides an enhanced ability to verify that the short-range transceiver is being used by an authorized user.

[0006a] According to an aspect of the present disclosure, there is provided a card verification system, comprising: a server configured to communicate over a network with a contactless card associated with a user, wherein the contactless cards stores first type data and second type data, wherein, after receipt of the first type data and second type data, the server is configured to: determine a first user identifier based on the first type data, determine a second user identifier based on the second type data, determine whether the first user identifier and the second user identifier both correspond to the contactless card associated with the user, and transmit a card verification message.

[0006b] According to another aspect of the present disclosure, there is provided a non-transitory computer-accessible medium containing executable instructions that, when executed

by a processing arrangement, cause the processing arrangement to perform procedures for card verification comprising: receiving, via a network, a card verification request to verify a contactless card, determining a first user identifier based on first type data; determining a second user identifier based on second type data; determining whether a first user identifier and a second user identifier both correspond to the contactless card associated with the user; and transmitting, via the network, a card verification message.

[0006c] According to another aspect of the present disclosure, there is provided a method for card verification, comprising: establishing a database storing user identifier information for a plurality of contactless cards; providing a contactless card configured for data communication via near field communication (NFC), the contactless card comprising a processor and a memory, the memory storing NFC data exchange format (NDEF) data, Europay Mastercard Visa (EMV) data, a first applet configured to provide the NDEF data responsive to an NDEF read request, and a second applet configured to provide the EMV data responsive to an EMV read request, wherein the contactless card is associated with a user; and providing a server in communication with the contactless card via a network, the server configured to receive the NDEF data and the EMV data and transmit a card verification message, the card verification message based on determining whether a first user identifier associated with the NDEF data and a second user identifier associated with the EMV data both correspond to the contactless card associated with the user.

[0007] Embodiments of the present disclosure provide a card verification system, comprising: a database storing user identifier information for a plurality of contactless cards; a contactless card comprising a processor and a memory, the memory storing first data of a first type, second data of a second type, a first applet configured to provide the first type data, and a second applet

configured to provide the second type data, wherein the contactless card is associated with a user; and a server configured to communicate over a network with the contactless card and the database; wherein, after entry into a short-range communication field, the contactless card is configured to transmit the first type data and the second type data to the server, and wherein, after receipt of the first type data and the second type data, the server is configured to: determine a first user identifier based on the first type data, determine a second user identifier

CLAIMS

1. A card verification system, comprising:
a server configured to communicate over a network with a contactless card associated with a user, wherein the contactless cards stores first type data and second type data,
wherein, after receipt of the first type data and second type data, the server is configured to:
determine a first user identifier based on the first type data,
determine a second user identifier based on the second type data,
determine whether the first user identifier and the second user identifier both correspond to the contactless card associated with the user, and
transmit a card verification message.
2. The card verification system of claim 1, further comprising:
the contactless card,
wherein the contactless card comprising a processor and a memory, the memory storing the first type data, the second data of a second type, a first applet configured to provide the first type data, and a second applet configured to provide the second type data,
and
wherein, after entry into a short-range communication field, the contactless card is configured to transmit the first type data and the second type data to the server.
3. The card verification system of claim 2, wherein

the short-range communication field comprises near field communication (NFC), and
the first type data comprises NFC data exchange format data.

4. The card verification system of claim 3, wherein:
the second type data comprises Europay Mastercard Visa (EMV) data, and
the client device stores a client application comprising instructions for execution by
the client device, and wherein the client application is further configured to transmit the
second type data to a card authorization network.
5. The card verification system of claim 3, further comprising:
a client device is associated with a point of sale (POS) system,
wherein the client device is configured to generate the short-range communication
field.
6. The card verification system of claim 6, wherein:
the card verification message indicates that the contactless card has been successfully
verified, and
the client device stores a client application comprising instructions for execution by
the client device, and wherein the client application is further configured to proceed with a
transaction using the contactless card.
7. The card verification system of claim 6, wherein:

the card verification message indicates that the contactless card has not been successfully verified, and

the client device stores a client application comprising instructions for execution by the client device, and wherein the client application is further configured to display an instruction to attempt verification using a different contactless card.

8. The card verification system of claim 1, further comprising:

a database storing user identifier information for a plurality of contactless cards, wherein the server is further configured to communicate over the network with the database.

9. A non-transitory computer-accessible medium containing executable instructions that, when executed by a processing arrangement, cause the processing arrangement to perform procedures for card verification comprising:

receiving, via a network, a card verification request to verify a contactless card,
determining a first user identifier based on first type data;
determining a second user identifier based on second type data;
determining whether a first user identifier and a second user identifier both correspond to the contactless card associated with the user; and
transmitting, via the network, a card verification message.

10. The non-transitory computer-accessible medium of claim 9, wherein:

the card verification request is generated in response to entry by the contactless card into a short-range communication field,

the card verification request is accompanied by first type data read from the contactless card and by second type data read from the contactless card, and

the contactless card is associated with a user.

11. The non-transitory computer-accessible medium of claim 9, wherein determining the first user identifier based on the first type data comprises searching a database using at least a portion of the first type data.

12. The non-transitory computer-accessible medium of claim 11, wherein determining the second user identifier based on the second type data comprises searching the database using at least a portion of the second type data.

13. The non-transitory computer-accessible medium of claim 12, wherein at least one of the first type data or the second type data comprises a key associated with the user.

14. The non-transitory computer-accessible medium of claim 13, further comprising using the key to authenticate the user.

15. The non-transitory computer-accessible medium of claim 9, wherein:
the short-range communication field comprises near field communication (NFC),
the first type data comprises NFC data exchange format data, and

the second type data comprises Europay Mastercard Visa (EMV) data.

16. The non-transitory computer-accessible medium of claim 15, further comprising:

transmitting the second type data to a card authorization network; and

receiving a transaction authorization response from the card authorization network.

17. A method for card verification, comprising:

establishing a database storing user identifier information for a plurality of contactless

cards;

providing a contactless card configured for data communication via near field

communication (NFC), the contactless card comprising a processor and a memory, the

memory storing NFC data exchange format (NDEF) data, Europay Mastercard Visa (EMV)

data, a first applet configured to provide the NDEF data responsive to an NDEF read request,

and a second applet configured to provide the EMV data responsive to an EMV read request,

wherein the contactless card is associated with a user; and

providing a server in communication with the contactless card via a network, the

server configured to receive the NDEF data and the EMV data and transmit a card

verification message, the card verification message based on determining whether a first user

identifier associated with the NDEF data and a second user identifier associated with the

EMV data both correspond to the contactless card associated with the user.

18. The method for card verification of claim 17, wherein determining the first user identifier based on the NDEF data comprises searching a database using at least a portion of the NDEF data.

19. The method for card verification of claim 18, wherein determining the second user identifier based on the EMV data comprises searching the database using at least a portion of the EMV data.

20. The method for card verification of claim 17, wherein at least one of the NDEF data or the EMV data comprises a key associated with the user.