

interaction with the portable device, traditional means of providing authentication and additional security are not effective.

[0004] There are some solutions that have emerged to address issues of authentication in remote transactions. One example is 3D Secure which allows entities such as Visa, MasterCard, and American Express to provide additional means to authenticate a portable device. For example, a password based method may be used which requires a user to register a password and then to input the password during each remote purchase transaction. This can be burdensome to the user whose payment experience may be interrupted to setup and register a password, and then to remember and enter the password for every remote transaction. Such a solution can also be expensive for a merchant or other entity to implement and maintain. Moreover, this solution can introduce other security issues. For example, password based solutions typically require a pop-up window to appear during the user's payment transaction. It may be difficult for the user to distinguish between a legitimate pop up window and a fraudulent phishing site. An inline frame may be used instead of a pop-up to reduce user confusion, but this may make it even harder for a user to verify that the inline frame is genuine. In addition, a user may not be allowed to proceed with a payment until they have registered a 3D Secure password. If a user does not want to risk providing the information during the purchase (or cannot remember the password), the user may have to cancel the transaction. Furthermore, many mobile browsers may not support inline frames or pop-ups and thus, the security feature may not work correctly on many mobile devices.

[0005] A more secure and effective way to authenticate users and portable devices is needed.

BRIEF SUMMARY

[0006] Embodiments of the invention are directed to systems, apparatuses, and methods to authenticate users and portable devices.

[0007]

According to a first aspect of the present invention, there is provided a method comprising: receiving, at a server computer, portable device information and a mobile device identifier associated with a mobile device; storing, by the server computer, the portable device information and the mobile device identifier in a database associated with the server computer; receiving, by the server computer, first transaction data from an access device for a physical or proximity transaction conducted at the access device, wherein the physical or proximity transaction includes physically presenting the portable device to the access device to provide portable device data to the access device; determining, by the server computer, from the first transaction data that the physical or proximity transaction is associated with the portable device; determining, by the server computer, a location of the access device; determining, by the server computer, a location of the mobile device associated with the mobile device identifier; determining, by the server computer, that the location of the mobile device matches the location of the access device; marking, by the server computer, the stored portable device information and the stored mobile device identifier as authentication verified; generating, by the server computer, a verification value or a digital certificate indicating that the status of the portable device is authentication verified; storing, by the server computer, the verification value or the digital certificate; receiving, at the server computer, second transaction data from a transactor computer for a remote transaction conducted via the transactor computer, wherein the remote transaction includes providing the portable device data to the transactor computer over a network without physically presenting the portable device to an access device; determining, by the server computer, from the second transaction data that the remote transaction is associated

with the portable device; determining, by the server computer, that the stored portable device information and the stored mobile device identifier are marked as authentication verified; identifying, by the server computer, the stored the verification value or the digital certificate; and sending, by the server computer, a message indicating the status of the portable device as authentication verified to the transactor computer or to an issuer, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.

[0008] According to a second aspect of the present invention, there is provided a server computer comprising: a processor; and a non-transitory computer readable medium coupled with the processor, the computer readable medium comprising instructions executable by the processor, the instructions comprising: receiving portable device information and a mobile device identifier associated with a mobile device; storing the portable device information and the mobile device identifier in a database associated with the server computer; receiving first transaction data from an access device for a physical or proximity transaction conducted at the access device, wherein the physical or proximity transaction includes physically presenting the portable device to the access device to provide portable device data to the access device; determining from the first transaction data that the physical or proximity transaction is associated with the portable device; determining a location of the access device; determining a location of the mobile device associated with the mobile device identifier; determining that the location of the mobile device matches

the location of the access device; marking the stored portable device information and the stored mobile device identifier as authentication verified; generating a verification value or a digital certificate indicating that the status of the portable device is authentication verified; storing the verification value or the digital certificate; receiving second transaction data from a transactor computer for a remote transaction conducted via the transactor computer, wherein the remote transaction includes providing the portable device data to the transactor computer over a network without physically presenting the portable device to an access device; determining from the second transaction data that the remote transaction is associated with the portable device; determining that the stored portable device information and the stored mobile device identifier are marked as authentication verified; identifying the stored the verification value or the digital certificate; and sending a message indicating the status of the portable device as authentication verified to the transactor computer or to an issuer, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.

[0009] According to a third aspect of the present invention, there is provided a computer apparatus comprising: a processor; and a non-transitory computer readable medium coupled with the processor, the computer readable medium comprising instructions executable by the processor, the instructions comprising: sending portable device

information and a mobile device identifier associated with a mobile device, to a server computer wherein the server computer stores the portable device information and the mobile device identifier in a database associated with the server computer; receiving first transaction data for a physical or proximity transaction conducted using the portable device, wherein the physical or proximity transaction includes physically presenting the portable device to an access device to provide portable device data to the access device; sending the first transaction data to the server computer wherein the server computer determines a location of an access device associated with the mobile device identifier, determines a location of the mobile device associated with the mobile device identifier, determines that the location of the mobile device identifier matches the location of the access device, marks the stored portable device information and the stored mobile device identifier in the database as authentication verified, generates a verification value or a digital certificate indicating that the status of the portable device is authentication verified, and stores the verification value or the digital certificate; receiving second transaction data for a remote transaction, wherein the remote transaction includes providing the portable device data over a network without physically presenting the portable device to the access device; and sending the second transaction data to the server computer wherein the server computer determines from the second transaction data that the remote transaction is associated with the portable device, determines that the stored portable device information the stored mobile device identifier are marked as authentication verified, identifies the stored the verification value or the digital certificate, and sends a message indicating the status of the portable device as authentication verified, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.

[0010] These and other embodiments of the invention are further described below.

BRIEF DESCRIPTION

[0011] FIG. 1 shows a block diagram of a system according to embodiments of the invention.

[0012] FIG. 2 shows a block diagram of an exemplary database according to embodiments of the invention.

[0013] FIG. 3 shows a block diagram of an exemplary server computer according to embodiments of the invention.

[0014] FIG. 4 shows a flowchart of a method according to embodiments of the invention.

[0015] FIG. 5 shows a flowchart of a method according to embodiments of the invention.

[0016] FIG. 6 shows a flowchart of a method according to embodiments of the invention.

[0017] FIG. 7 shows an exemplary device according to embodiments of the invention.

[0018] FIG. 8 shows an exemplary computer system according to embodiments of the invention.

DETAILED DESCRIPTION

[0019] Embodiments of the invention are directed to systems, apparatuses, and methods to authenticate portable devices. For example, a user may provide information to register a portable device for authentication of remote transactions (e.g., primary account number (PAN), expiry date for the portable device, a card verification value (CVV), etc.). The user may also provide a mobile device identifier (e.g., a mobile phone number). The user may provide this information to a

CLAIMS

1. A method comprising:
 - receiving, at a server computer, portable device information and a mobile device identifier associated with a mobile device;
 - storing, by the server computer, the portable device information and the mobile device identifier in a database associated with the server computer;
 - receiving, by the server computer, first transaction data from an access device for a physical or proximity transaction conducted at the access device, wherein the physical or proximity transaction includes physically presenting the portable device to the access device to provide portable device data to the access device;
 - determining, by the server computer, from the first transaction data that the physical or proximity transaction is associated with the portable device;
 - determining, by the server computer, a location of the access device;
 - determining, by the server computer, a location of the mobile device associated with the mobile device identifier;
 - determining, by the server computer, that the location of the mobile device matches the location of the access device;
 - marking, by the server computer, the stored portable device information and the stored mobile device identifier as authentication verified;
 - generating, by the server computer, a verification value or a digital certificate indicating that the status of the portable device is authentication verified;
 - storing, by the server computer, the verification value or the digital certificate;
 - receiving, at the server computer, second transaction data from a transactor computer for a remote transaction conducted via the transactor computer, wherein the remote transaction includes providing the portable device data to the transactor computer over a network without physically presenting the portable device to an access device;
 - determining, by the server computer, from the second transaction data that the remote transaction is associated with the portable device;
 - determining, by the server computer, that the stored portable device information and the stored mobile device identifier are marked as authentication verified;
 - identifying, by the server computer, the stored the verification value or the digital certificate; and
 - sending, by the server computer, a message indicating the status of the portable device as authentication verified to the transactor computer or to an issuer, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.

2. The method of claim 1 wherein determining the location of the access device includes determining the location of the access device from location information included in the transaction data.
3. The method of claim 1 wherein determining the location of the mobile device includes sending a message to the mobile device requesting information to confirm the location of the mobile device.
4. The method of claim 3 wherein requesting information includes a request for confirmation for a recent transaction or a challenge question.
5. The method of claim 1 wherein determining the location of the mobile device includes utilizing location technology to determine the geographical position of the mobile device.
6. The method of claim 1 wherein storing the information for the portable device that includes the mobile device identifier further comprises indicating that the stored information for the portable device is not yet authentication verified.
7. The method of claim 1, wherein the portable device information and the mobile device identifier are provided by a user during an initial transaction before the physical or proximity transaction.
8. The method of claim 1, wherein the portable device information and the mobile device identifier are provided by a user via an electronic wallet.
9. The method of claim 1 wherein the message indicating the status of the portable device as authentication verified is sent to the transactor computer, and wherein the method further comprises:
 - receiving, at the server computer, from the transactor computer, an authorization request message for the remote transaction, the authorization request message including the verification value or the digital certificate;
 - determining, by the server computer, that the remote transaction is authentic based on the verification value or the digital certificate; and
 - forwarding, by the server computer, to the issuer, the authorization request message for the remote transaction including the verification value or the digital certificate, wherein the issuer authorizes the remote transaction based on the verification value or the digital certificate.

10. The method of claim 1, wherein storing the portable device information and the mobile device identifier in a database associated with the server computer causes the mobile device to be associated with the portable device at the server computer, wherein the remote transaction associated with the portable device is initiated via the mobile device, and wherein the remote transaction is considered an authentication verified transaction because it is initiated via the mobile device and the mobile device is verified as being associated with the portable device.

11. The method of claim 1, wherein marking the stored portable device information and the stored mobile device identifier as authentication verified indicates that an association between the mobile device and portable device is verified, and that the portable device is eligible for use in remote transactions without having to check or compare a physical location.

12. The method of claim 1, wherein a physical transaction is a contact transaction, and wherein a proximity transaction is a contactless NFC transaction.

13. A server computer comprising:

- a processor; and

- a non-transitory computer readable medium coupled with the processor, the computer readable medium comprising instructions executable by the processor, the instructions comprising:

- receiving portable device information and a mobile device identifier associated with a mobile device;

- storing the portable device information and the mobile device identifier in a database associated with the server computer;

- receiving first transaction data from an access device for a physical or proximity transaction conducted at the access device, wherein the physical or proximity transaction includes physically presenting the portable device to the access device to provide portable device data to the access device;

- determining from the first transaction data that the physical or proximity transaction is associated with the portable device;

- determining a location of the access device;

- determining a location of the mobile device associated with the mobile device identifier;

- determining that the location of the mobile device matches the location of the access device;

- marking the stored portable device information and the stored mobile device identifier as authentication verified;

generating a verification value or a digital certificate indicating that the status of the portable device is authentication verified;

storing the verification value or the digital certificate;

receiving second transaction data from a transactor computer for a remote transaction conducted via the transactor computer, wherein the remote transaction includes providing the portable device data to the transactor computer over a network without physically presenting the portable device to an access device;

determining from the second transaction data that the remote transaction is associated with the portable device;

determining that the stored portable device information and the stored mobile device identifier are marked as authentication verified;

identifying the stored the verification value or the digital certificate; and

sending a message indicating the status of the portable device as authentication verified to the transactor computer or to an issuer, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.

14. The server computer of claim 13 wherein determining the location of the access device includes determining the location of the access device from location information included in the transaction data.

15. The server computer of claim 13 wherein determining the location of the mobile device includes sending a message to the mobile device requesting information to confirm the location of the mobile device.

16. The server computer of claim 13 wherein requesting information includes a request for confirmation for a recent transaction or a challenge question.

17. The server computer of claim 13 wherein determining the location of the mobile device includes utilizing location technology to determine the geographical position of the mobile device.

18. The server computer of claim 13 wherein storing the information for the portable device that includes the mobile device identifier further comprises indicating that the stored information for the portable device is not yet authentication verified.

19. The server computer of claim 13 wherein the access device is an electronic cash register.

20. A computer apparatus comprising:

a processor; and

a non-transitory computer readable medium coupled with the processor, the computer readable medium comprising instructions executable by the processor, the instructions comprising:

sending portable device information and a mobile device identifier associated with a mobile device, to a server computer wherein the server computer stores the portable device information and the mobile device identifier in a database associated with the server computer;

receiving first transaction data for a physical or proximity transaction conducted using the portable device, wherein the physical or proximity transaction includes physically presenting the portable device to an access device to provide portable device data to the access device;

sending the first transaction data to the server computer wherein the server computer determines a location of an access device associated with the mobile device identifier, determines a location of the mobile device associated with the mobile device identifier, determines that the location of the mobile device identifier matches the location of the access device, marks the stored portable device information and the stored mobile device identifier in the database as authentication verified, generates a verification value or a digital certificate indicating that the status of the portable device is authentication verified, and stores the verification value or the digital certificate;

receiving second transaction data for a remote transaction, wherein the remote transaction includes providing the portable device data over a network without physically presenting the portable device to the access device; and

sending the second transaction data to the server computer wherein the server computer determines from the second transaction data that the remote transaction is associated with the portable device, determines that the stored portable device information the stored mobile device identifier are marked as authentication verified, identifies the stored the verification value or the digital certificate, and sends a message indicating the status of the portable device as authentication verified, the message including the verification value or the digital certificate, wherein the verification value or the digital certificate is subsequently used in a determination as to whether the remote transaction is fraudulent.