

**SECURE AUTHENTICATION BASED ON IDENTITY DATA STORED IN A
CONTACTLESS CARD**

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 16/726,385, titled “SECURE AUTHENTICATION BASED ON IDENTITY DATA STORED IN A CONTACTLESS CARD” filed on December 24, 2019. The contents of the aforementioned application are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] Embodiments herein generally relate to computing platforms, and more specifically, to using a contactless card storing identity data for secure authentication.

BACKGROUND

[0003] Identity verification is an important task for modern computing systems. Conventional approaches may require that users provide additional information, such as a one-time passcode (OTP), when attempting to access computing systems or perform electronic transactions. However, security vulnerabilities may exist in these solutions. For example, the OTP may be intercepted and used to gain unauthorized access. Furthermore, different systems may require different types of additional information for identity verification, making conventional solutions impractical for many users.

SUMMARY

[0003a] According to an aspect, there is provide a computer-implemented method comprising: receiving, by an application executing on a processor of a device, a request to perform an operation associated with an account; receiving, by the application, encrypted data from a contactless card associated with the account; receiving, by the application from an authentication server, a decryption result; determining, by the application based on the decryption result, that the authentication server decrypted the encrypted data; determining, by the application, a type of authentication data required to

authorize the operation; receiving, by the application based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image; determining, by the application, that the first data element satisfies at least one rule for authorizing the operation; authorizing, by the application, performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and performing the operation by the application based on the authorization.

[0003b] According to another aspect, there is provided a computer-readable storage medium storing computer-readable program code executable by a processor of a device to cause the processor to: receive a request to perform an operation associated with an account; receive encrypted data from a contactless card associated with the account; receive, from an authentication server, a decryption result; determine, based on the decryption result, that the authentication server decrypted the encrypted data; determine a type of authentication data required to authorize the operation; receive, based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image; determine that the first data element satisfies at least one rule for authorizing the operation; authorize performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and perform the operation based on the authorization.

[0003c] According to another aspect, there is provided a system comprising: a processor and a memory storing instructions which when executed by the processor cause the processor to: receive a request to perform an operation associated with an account; receive encrypted data from a contactless card associated with the account; receive, from an authentication server, a decryption result; determine, based on the decryption result, that the authentication server decrypted the encrypted data; determine a type of authentication data required to authorize the operation; receive, based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image; determine that the first data element satisfies at least one rule for authorizing the operation; authorize performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and perform the operation based on the authorization.

[0004] Embodiments disclosed herein provide systems, methods, articles of manufacture, and computer-readable media for secure authentication based on identity data stored in a contactless card. In one example, an application may receive an indication

CLAIMS

1. A computer-implemented method, comprising:

- receiving, by an application executing on a processor of a device, a request to perform an operation associated with an account;
- receiving, by the application, encrypted data from a contactless card associated with the account;
- receiving, by the application from an authentication server, a decryption result;
- determining, by the application based on the decryption result, that the authentication server decrypted the encrypted data;
- determining, by the application, a type of authentication data required to authorize the operation;
- receiving, by the application based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image;
- determining, by the application, that the first data element satisfies at least one rule for authorizing the operation;
- authorizing, by the application, performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and
- performing the operation by the application based on the authorization.

2. The method of claim 1, further comprising:

- transmitting, by the application, the encrypted data to the authentication server;
- and
- determining, by the application, the type of authentication data based on a type of the operation and at least one rule for the type of the operation.

3. The method of claim 1, further comprising:

- receiving, by the application, a first image of a person captured by an image capture device of the device;
- comparing, by the application, the first image to the passport image or the driver license image; and

determining, by the application based on the comparison, that a similarity of a person in the passport image or the driver license image and the person in the first image exceeds a similarity threshold, wherein the determination the passport image or the driver license image satisfies the at least one rule is based on the similarity exceeding the similarity threshold.

4. The method of claim 3, wherein the similarity threshold is based on a type of the operation and at least one rule for the type of the operation, the method further comprising:

determining, by the application based on the similarity exceeding the similarity threshold, that the person in the first image matches the person in the passport image.

5. The method of claim 1, wherein the first data element is encrypted when received from the contactless card, the method further comprising:

transmitting, by the application, the encrypted first data element to the authentication server; and

receiving, by the application, an unencrypted version of the first data element from the authentication server.

6. The method of claim 1, wherein the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, (iii) accessing a page of the application, or (iv) processing a transaction using the contactless card.

7. The method of claim 1, further comprising:

receiving, by the application from the contactless card, a digital signature of the first data element; and

verifying, by the application, the digital signature based on a public key for the contactless card.

8. A computer-readable storage medium storing computer-readable program code executable by a processor of a device to cause the processor to:

receive a request to perform an operation associated with an account;

receive encrypted data from a contactless card associated with the account;

receive, from an authentication server, a decryption result;

determine, based on the decryption result, that the authentication server decrypted the encrypted data;

determine a type of authentication data required to authorize the operation;

receive, based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image;

determine that the first data element satisfies at least one rule for authorizing the operation;

authorize performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and

perform the operation based on the authorization.

9. The computer-readable storage medium of claim 8, storing computer-readable program code executable by the processor to cause the processor to:

transmit the encrypted data to the authentication server; and

determine the type of authentication data based on a type of the operation and at least one rule for the type of the operation.

10. The computer-readable storage medium of claim 8, storing computer-readable program code executable by the processor to cause the processor to:

receive a first image of a person captured by an image capture device of the device;

compare the first image to the passport image or the driver license image; and

determine, based on the comparison, that a similarity of a person in the passport image or the driver license image and the person in the first image exceeds a similarity threshold, wherein the determination the passport image or the driver license image satisfies the at least one rule is based on the similarity exceeding the similarity threshold.

11. The computer-readable storage medium of claim 10, wherein the similarity threshold is based on a type of the operation and at least one rule for the type of the operation, the medium storing computer-readable program code executable by the processor to cause the processor to:

determine, based on the similarity exceeding the similarity threshold, that the person in the first image matches the person in the passport image.

12. The computer-readable storage medium of claim 8, wherein the first data element is encrypted when received from the contactless card, the medium storing computer-readable program code executable by the processor to cause the processor to:

- transmit the encrypted first data element to the authentication server; and
- receive an unencrypted version of the first data element from the authentication server.

13. The computer-readable storage medium of claim 8, wherein the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, or (iii) processing a transaction using the contactless card.

14. The computer-readable storage medium of claim 8, storing computer-readable program code executable by the processor to cause the processor to:

- receive, from the contactless card, a digital signature of the first data element; and
- verify the digital signature based on a public key for the contactless card.

15. A system, comprising:

- a processor; and
- a memory storing instructions which when executed by the processor cause the processor to:
 - receive a request to perform an operation associated with an account;
 - receive encrypted data from a contactless card associated with the account;
 - receive, from an authentication server, a decryption result;
 - determine, based on the decryption result, that the authentication server decrypted the encrypted data;
 - determine a type of authentication data required to authorize the operation;
 - receive, based on the determined type of authentication data, a first data element from the contactless card, the first data element comprising a passport image or a driver license image;
 - determine that the first data element satisfies at least one rule for authorizing the operation;

authorize performance of the operation based on the decryption result and the determination that the first data element satisfies the at least one rule for authorizing the operation; and
perform the operation based on the authorization.

16. The system of claim 15, the memory storing instructions which when executed by the processor cause the processor to:

transmit the encrypted data to the authentication server; and
determine the type of authentication data based on a type of the operation and at least one rule for the type of the operation.

17. The system of claim 15, the memory storing instructions which when executed by the processor cause the processor to:

receive a first image of a person captured by an image capture device of the system;
compare the first image to the passport image or the driver license image; and
determine, based on the comparison, that a similarity of a person in the passport image or the driver license image and the person in the first image exceeds a similarity threshold, wherein the determination the passport image or the driver license image satisfies the at least one rule is based on the similarity exceeding the similarity threshold.

18. The system of claim 17, wherein the similarity threshold is based on a type of the operation and at least one rule for the type of the operation, the memory storing instructions which when executed by the processor cause the processor to:

determine, based on the similarity exceeding the similarity threshold, that the person in the first image matches the person in the passport image.

19. The system of claim 15, wherein the first data element is encrypted when received from the contactless card, the memory storing instructions which when executed by the processor cause the processor to:

transmit the encrypted first data element to the authentication server; and
receive an unencrypted version of the first data element from the authentication server.

20. The system of claim 15, wherein the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, or (iii) processing a transaction using the contactless card.