processing, and significantly increases overall system complexity required to process a transaction from end to end.

BRIEF SUMMARY

[0006] According to a first aspect, there is provided a system for processing a digital transaction including: a user authenticator configured to: receive biometric data associated with a user, wherein the biometric data is received from a sensor, and the sensor corresponds to at least one of: an image sensor, a finger print sensor, a user interaction pattern sensor, and an infrared image sensor; receive user identifying information; determine whether the biometric data associated with the user is associated with the user identifying information; validate the user based on the user identifying information; and generate user credentials when the user is validated, the user credentials associated with the user; a processor in communication with the user authenticator; and non-transitory computer readable media that stores instruction code that when executed by the processor causes the processor to: receive the user credentials; determine different categories of information required to process the digital transaction; determine one or more data source systems, wherein the data source systems stores information related to the different categories of information and the user identifying information; aggregate, from one or more data source systems, the information associated with the user identifying information; communicate the aggregated information to a processing system, wherein the processing system is configured to process the digital transaction; determine a trust level for one or more categories of the categories of information; determine whether user information associated with a first category of the categories of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and when the trust level is below the predetermined trust level, control the input/output processor to communicate a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category.

[0007] According to a second aspect, there is provided a method for processing a digital transaction including: receiving, from a user terminal that includes a sensor, biometric data associated with a user, the sensor corresponding to at least one of: an image sensor, a finger print sensor, a user interaction pattern sensor, and an infrared image sensor; receiving user identifying information; determining whether the biometric data associated with the user is associated with the user identifying information; validating the user based on the user identifying information; and generating user credentials associated with the user when the user is validated; receiving the user credentials; determining different categories of information required to process the digital transaction; determining one or more data source systems that store information related to the different categories of information and with the user identifying information; aggregating, from the one or more data source systems, the information associated with the user identifying information; and communicating the aggregated information to a

processing system to thereby process the digital transaction; wherein aggregating the information associated with the different categories further comprises determining a trust level for one or more categories of the categories of information; determining whether user information associated with a first category of the categories of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and when the trust level is below the predetermined trust level, communicating a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category of information.

[0008] According to a third aspect, there is provided a non-transitory computer readable media that stores instruction code for processing a transaction, the instruction code being executable by a machine for causing the machine to perform acts including: receiving, from a user terminal that includes the sensor, biometric data associated with a user; receiving user identifying information; determining whether the biometric data associated with the user is associated with the user identifying information to thereby validate the user; and if the user is validated, generating user credentials associated with the user; receiving the user credentials; determining different categories of information required to process the digital transaction; determining one or more data source systems that store information related to the different categories of information and the user identifying information; aggregating, from the one or more data source systems, the information associated with the user identifying information; communicating the aggregated information to a processing system to thereby process the digital transaction; determine a trust level for one or more categories of the categories of information determine whether user information associated with a first category of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and when the trust level is below the predetermined trust level, communicate a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category of information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Fig. 1 illustrates an exemplary environment that includes various entities that facilitate processing a digital transaction;

[0010] Fig. 2 illustrates an exemplary transaction data aggregation and trust assurance system of the environment;

[0011] Figs. 3 and 4 illustrate operations performed by various entities of the environment in processing a digital transaction;

identifying information 502 (Fig. 5) that facilitates locating information related to the user in databases of various data sources

[0031] In one implementation, the user's identity may be confirmed based on one or more identification documents such as a photo ID, government ID, etc. For example, various image processing techniques may be performed to identify an image of an individual on the identification document (Fig. 5, 505) and to compare the image with an image of the user to determine whether the individual pictured on the identification document is the user.

[0032] In some implementations, the user authenticator 210 may be configured to perform the various operations above and/or configured to operate in conjunction with one or more 3rd party services 115 such as CatfishAIR® by AuthenticID® in making these determinations. In other implementations, confirmation of the identity of the user may be performed entirely by 3rd party services.

[0033] Other types of user information are contemplated. For example, the user authenticator may be configured to receive biometric information, such as biometric information associated with one or more finger prints, facial infrared scans, etc., to authenticate the user of the user terminal. In this regard, the user terminal may be configured with, for example, a sensor such as a finger print sensor, infrared imager sensor, etc. Biometric information associated with the user may have been previously obtained. For example, biometric information may have been obtained by and stored on a 3rd party service system 115, a data source system 110 or a different system in communication with the DATAS 102. In addition or alternatively, the information may have been obtained by and stored by the DATAS 102.

[0034] The processor 215 may correspond to a stand-alone computer system such as an Intel®, AMD®, or PowerPC® based computer system or a different computer system and can include application specific computer systems. The computer systems may include an operating system, such as Microsoft Windows®, Linux, Unix® or other operating system.

[0035] It is contemplated that the I/O processor 205, user authenticator 210, and any other subsystem referenced herein may correspond to a stand-alone computer system

CLAIMS

1. A system for processing a digital transaction comprising:

a user authenticator configured to:

receive biometric data associated with a user, wherein the biometric data is received from a sensor, and the sensor corresponds to at least one of: an image sensor, a finger print sensor, a user interaction pattern sensor, and an infrared image sensor;

receive user identifying information;

determine whether the biometric data associated with the user is associated with the user identifying information;

validate the user based on the user identifying information; and

generate user credentials when the user is validated, the user credentials associated with the user;

a processor in communication with the user authenticator; and

non-transitory computer readable media that stores instruction code that when executed by the processor causes the processor to:

receive the user credentials;

determine different categories of information required to process the digital transaction;

determine one or more data source systems, wherein the data source systems stores information related to the different categories of information and the user identifying information;

aggregate, from one or more data source systems, the information associated with the user identifying information;

communicate the aggregated information to a processing system, wherein the processing system is configured to process the digital transaction;

determine a trust level for one or more categories of the categories of information;

determine whether user information associated with a first category of the categories of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and

when the trust level is below the predetermined trust level, control the input/output processor to communicate a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category.

2. The system according to claim 1, wherein the system further comprises an input/output processor, wherein the instruction code causes the processor to:

control the input/output processor to:

generate an interface that facilitates receiving user identifying information and scanning an identification document with the image sensor; and

communicate the interface to the user terminal;

receive the user identifying information and image data from the image sensor associated with the identification document;

identify textual images in the image data; and

convert the textual images in the image data to text information, wherein the text information facilitates processing the digital transaction.

3. The system according to claim 2, wherein the identification document includes an image of an individual associated with the identification document, wherein the interface is further configured to control the sensor of the user terminal to capture an image of the user, and wherein the instruction code causes the processor to compare the image of the user with the image of the individual associated with the identification document to determine whether the user of the user terminal is the individual.

4. The system according to claim 1, wherein the instruction code causes the processor to:

receive, via the input/output processor and from the processing system, a listing that identifies categories of information required to process the transaction.

5. The system according to claim 1, wherein prior to communicating the aggregated information to the processing system, the aggregated information is communicated to the user terminal to facilitate review and acceptance of the aggregated information by the user.

6. The system according to claim 1, wherein prior to aggregating, from the one or more data source systems, the information associated with the user, a request for consent to obtain the information is communicated to the user terminal to thereby grant a user of the user terminal control over whether the information associated with the user can be aggregated.

7. A method for processing a digital transaction comprising:

receiving, from a user terminal that includes a sensor, biometric data associated with a user,

the sensor corresponding to at least one of: an image sensor, a finger print sensor, a user interaction pattern sensor, and an infrared image sensor;

receiving user identifying information;

determining whether the biometric data associated with the user is associated with the user identifying information;

validating the user based on the user identifying information; and

generating user credentials associated with the user when the user is validated;

receiving the user credentials;

determining different categories of information required to process the digital transaction;

determining one or more data source systems that store information related to the different categories of information and with the user identifying information;

aggregating, from the one or more data source systems, the information associated with the user identifying information; and

communicating the aggregated information to a processing system to thereby process the digital transaction;

wherein aggregating the information associated with the different categories further comprises determining a trust level for one or more categories of the categories of information;

determining whether user information associated with a first category of the categories of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and

when the trust level is below the predetermined trust level, communicating a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category of information.

8. The method according to claim 7, wherein receiving information that identifies the user further comprises:

generating an interface that facilitates receiving user identifying information and scanning an identification document with the image sensor;

communicating the interface to the user terminal;

receiving, from the user terminal and via the interface, the user identifying information and image data from the image sensor associated with the identification document;

identifying textual images in the image data; and

converting textual images defined in the image data into text information, wherein the text information facilitates processing the digital transaction.

9. The method according to claim 8, wherein the authenticated ID includes an image of an individual associated with the authenticated ID, wherein the interface is further configured to control the sensor of the user terminal to capture an image of the user, and wherein the method further comprises comparing the image of the user with the image of the individual associated with the identification document to determine whether the user of the user terminal is the same person as the individual.

10. The method according to claim 7, wherein determining the different categories of information required to process the digital transaction further comprises receiving, from the processing system, a listing of the different categories of information required to process the transaction.

11. The method according to claim 7, wherein prior to communicating the aggregated information to the processing system, the aggregated information is communicated to the user terminal to facilitate review and acceptance of the aggregated information by the user.

12. A non-transitory computer readable media that stores instruction code for processing a transaction, the instruction code being executable by a machine for causing the machine to perform acts including:

receiving, from a user terminal that includes the sensor, biometric data associated with a user;

receiving user identifying information;

determining whether the biometric data associated with the user is associated with the user identifying information to thereby validate the user; and

if the user is validated, generating user credentials associated with the user;

receiving the user credentials;

determining different categories of information required to process the digital transaction;

determining one or more data source systems that store information related to the different categories of information and the user identifying information;

aggregating, from the one or more data source systems, the information associated with the user identifying information;

communicating the aggregated information to a processing system to thereby process the digital transaction;

determine a trust level for one or more categories of the categories of information

determine whether user information associated with a first category of information, received from a first data source system of the one or more data source systems, is below a predetermined trust level; and

when the trust level is below the predetermined trust level, communicate a second interface to the user terminal that requests the user of the user terminal to provide the information associated with the first category of information.

13. The non-transitory computer readable media according to claim 12, wherein the instruction code causes the machine to:

generate an interface that facilitates receiving user identifying information and scanning an identification document with the image sensor;

communicate the interface to the user terminal;

receive the user identifying information and image data from the image sensor associated with the identification document from the user terminal via the interface; and

convert textual images defined in the image data into text information, wherein the text information facilitates processing the digital transaction.

14. The non-transitory computer readable media according to claim 13, wherein the identification document includes an image of an individual associated with the identification document, wherein the interface is further configured to control the sensor of the user terminal to capture an image of the user, and wherein the instruction code causes the machine to compare the image of the user with the image of the individual associated with the authenticated ID to determine whether the user of the user terminal is the same person as the individual.

15. The non-transitory computer readable media according to claim 12, wherein the instruction code causes the machine to receive, from the processing system, a listing of the different categories of information required to process the transaction.