

SYSTEM AND METHOD FOR MANAGING ASSOCIATIONS IN AN ONLINE NETWORK

TECHNICAL FIELD

[001] This disclosure relates to generally, to computer-based real time information exchange, and, more particularly, to moderated online dating, virtual dating and offline matchmaking services.

BACKGROUND

[002] Online dating services have been heavily used worldwide by single individuals to find their potential romantic partners and even spouses. The economically and physically convenient access to the service via cell phones and desktops/laptops and internet, such matchmaking method has been extremely popular in recent few decades. However, due to the identity and verification issues, online dating is fraught with issues related to fake profiles, false statements, misrepresentations and duplicity of membership. These result in significant online dating frauds rates, emotional breakdown rates as well as financial losses rates increase year over year across the globe. Moreover, the recommendations from existing online platforms are not up to the mark and result in low dating satisfaction rates and higher dating failure rates due to mismatch in characteristics, personality and many other important personal traits of two individuals.

[003] Conventionally, online dating sites do not verify the authenticity of users and this was clearly stated in their Terms of Service. Only some offline matchmaking companies require government issued identification information to register in their internal system to be manually matched. Further, some of them use manual curators to offer personalized or custom selected profiles for association.

[004] However, use of manual curators may not provide the best recommendations since the limitation on human ability to match multiple data points. Further, such recommendations may not be provided in real-time based on manual operations. Furthermore, identification checks may fail to identify frauds due to lack of verifying data. Lastly, the issue of fake profile pictures might not get solved based on manual checks.

[005] In light of above mentioned problems, there does not exist a solution that provides a risk free and authentic and efficient system and method to make and manage associations on an online platform such as a mobile phone to search for and communicate with desirable acquaintances at local social locations and to increase real-time engagement between a plurality of users.

SUMMARY

[006] The present disclosure seeks to provide a system and a computer implemented method for managing associations between a plurality of

entities in a safe, reliable, effective and efficient manner. The system leverages biometric authentication and identity verification to ensure authentic entity profiles and weed out fake profiles and transactions. Further, the system employs one or more artificial intelligence based algorithms to generate an integrity score for a registered entity based on veracity of information shared by an entity with other entities on the platform, thereby eliminating fake claims made by registered entities to solicit proposals and connection requests.

[007] Embodiments of the present disclosure substantially eliminate or at least partially address the aforementioned problems.

[008] Additional aspects, advantages, features and objects of the present disclosure would be made apparent from the drawings and the detailed description of the illustrative embodiments construed in conjunction with the appended claims that follow.

[009] It will be appreciated that features of the present disclosure are susceptible to being combined in various combinations without departing from the scope of the present disclosure as defined by the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The summary above, as well as the following detailed description of illustrative embodiments are better understood when read in conjunction

with the appended drawings. For the purpose of illustrating the present disclosure, exemplary constructions of the disclosure are shown in the drawings. However, the present disclosure is not limited to specific methods and instrumentalities disclosed herein. Moreover, those in the art will understand that the drawings are not to scale. Wherever possible, like elements have been indicated by identical numbers.

[0011] Embodiments of the present disclosure will now be described, by way of example only, with reference to the following diagrams wherein:

[0012] **FIG. 1** illustrates a block diagram of an example system according to the present disclosure.

[0013] **Fig. 2** depicts a network graph as per the preferred embodiment of the present invention.

[0014] Fig. 3 depicts a flowchart describing the method steps as per a preferred embodiment of the present invention.

[0015] It will be appreciated that the drawings illustrated herein are for representation purposes only and do not intend to limit the scope of the present disclosure, and actual implementation of the present disclosure may be viewed substantially differently.

DETAILED DESCRIPTION

[0016] The following description illustrates embodiments of the present disclosure and ways in which they can be implemented. Although some modes of carrying out the present disclosure have been disclosed, those skilled in the art would recognize that other embodiments for carrying out or practicing the present disclosure are also possible.

[0017] The present invention discloses a system and a computer implemented method for managing associations between a plurality of entities in a safe, reliable, effective and efficient manner. The system leverages biometric authentication and identity verification to ensure authentic entity profiles and weed out fake profiles and transactions. Further, the system employs one or more artificial intelligence based algorithms to generate an integrity score for a registered entity based on veracity of information shared by an entity with other entities of the platform, thereby eliminating fake claims made by registered entities to solicit proposals and connection requests.

[0018] **FIG. 1** illustrates a block diagram of an example system according to the present disclosure, for implementation of a system for managing associations in an online network **100** according to the present disclosure. The system **100** comprises a processing unit **102** communicably coupled, via

a data communication network **108**, to a biometric server **104** and a database arrangement **106**. The processing unit further comprises a memory **110** to store executable instructions. The system further comprises an identity server **112** in communication with a blockchain configured to store one or more user credentials.

[0019] In an aspect of the present invention, the processing unit **102** is configured to accept a request for registration from a plurality of entities. In a preferred embodiment, the entities are individuals looking to solicit and/or offer connection to, and from, other individuals. Each of the plurality of entities may register with the system through their respective client devices 114a1, 114a2, 114a3 (collectively "**client devices 114**"), The processing unit **102** is operable to generate a registration link accessible by the entities through a web browser or a mobile application on their respective client devices **114**.

[0020] Each of the plurality of entities willing to register with the system **100** is required to submit information that is used by the processing unit **102** to create an entity profile wherein the entity profile is distinct for each of the plurality of entities. The registration of an entity with the system requires the entity to submit personal information, through a graphical user interface associated with the client device, such as name, username, address, current address, professional qualifications, a recent picture as profile image, social

security number etc. The processing unit **102** is operable to generate a unique identifier for each entity profile based on the submitted personal information. Further, each of the plurality of entities is required to submit information and preferences related to personality traits, sexual compatibility, and behavioral aspects. Moreover, similar preferences and information related to potential partners is also collected from the entity and saved as desired partner traits. In an embodiment, said information is collected by means of a questionnaire with input from the entity registering with the system. Optionally, said information may be determined by the processing unit **102** through performance of the entity in one or more visual tests offered through the graphical user interface of the client devices. Said information and preferences are stored in the entity profile in the form of one or more attributes. Optionally, in some embodiments, an entity may be required to submit genomic data and DNA samples as a part of the entity profile. Furthermore, an entity is requested for preconfigured permissions to access one or more social media profiles associated with the entity.

[0021] The processing unit **102** is further operable to store the entity profile along with the unique identifier in the database arrangement. Any information related to the entity may be retrieved by the processing unit **102**. In a preferred embodiment of the present invention, the plurality of entities is saved in form of a network graph in the database arrangement wherein the network graph comprises pre-identified connections for the plurality of

entities, based on the entity profile for each of the plurality of entities. Each node of the network graph represents an entity registered with the system and the edges between the nodes represent relationships between the entities. Said relationships may be direct or inferred. Edges in the form of direct relationship may be formed based on a two-way communication between the two entities. Optionally, edges in the form of direct relationships may also be formed based on a positive response gesture on the entity profile of one entity by the other entity. Further, edges in the form of inferred relationships are formed based on connection between the two entities on one or more social media handles. As an example, if the two entities follow each other on Twitter or LinkedIn, that creates an inferred relationship between them. **Fig. 2** depicts a network graph as per the present disclosure.

[0022] In an embodiment of the present invention, the processing unit **102** is configured to authenticate an entity through one or more biometric recognition methods. The one or more biometric recognition methods could be one of a face recognition, fingerprint scan, retina scan or a combination of two or more methods. The biometric recognition helps in weeding out fake entity profiles or duplicate entity profiles from the system. The entity registering with the system is required to submit at least one biometric data through a biometric device coupled to the client device **114**. Said biometric data is stored within a biometric server communicably coupled to the processing unit **102** and associated with the unique identifier of the entity

profile corresponding to the entity. In a preferred embodiment of the present invention, the biometric data is a facial image of the entity. The processing unit is operable to compare the facial image captured through the biometric recognition means with the current profile picture of the entity in the entity profile to assess whether both of them relate to the same entity. The processing unit is operable to analyze one or more facial features from the captured biometric facial data and the submitted current profile picture, compare said facial features and derive a match score for the entity. If the match score is above a given threshold, the processing unit determines that the entity is authentic. This helps in eliminating the issue of fake profile images used by one or more entities. In yet another embodiment of the present invention, said biometric data is used for payment processing for one or more services available to the entity on the system.

[0023] The processing unit **102** is communicably coupled to a blockchain ledger wherein the blockchain ledger comprises validated information from one or more government and professional institutes. Any information related to professional qualification or identity may be cross validated, by the identity server **112**, through the blockchain ledger. Optionally, in another embodiment, the entity profile associated with each of the plurality of entities is saved in the blockchain and an audit trail is maintained for changes made by the entity to its entity profile. Therefore, any user may validate, through the identity server **112**, information about the past associations of a

particular entity and whether an entity has lied about his past associations and relationships. This results in transparency in communications and information symmetry between entities registered with the system **100**.

[0024] Optionally, the plurality of entities are classified into one or more tiers based on entity profile information and an assessment report wherein different levels of services are provided to entities based on their designated tier. As an example a Tier-IV registered entity shall have priority service as compared to a Tier-I user. The assessment report is based on manual background checks and authentication and added to the entity profile. In an embodiment, direct communication between entities associated with different tiers may be prohibited based on security settings of an entity profile or based on such a selection made by the entity through their graphical user interface.

[0025] In an aspect of the present invention, the processing unit **102** is further operable to determine an importance score for each of the nodes in relation to a given node. The importance score is based on a correlation of one or more attributes from the entity profile of two nodes. As an example, the correlation may be based upon similar work profiles, personality traits of being extrovert or in some cases behavioral traits of being humorous or likes and dislikes such as travelling etc. The importance score is calculated on the basis of information available on the entity profile from the time of registration and the desired partner traits as provided. Throughout this disclosure, an

importance score in relation to other nodes signifies a compatibility level of a node with the other nodes i.e. entities. Higher the importance score, higher is the compatibility level. In an embodiment of the present invention, the importance score is determined on the basis of one or more specific attributes selected by an entity.

[0026] In yet another aspect of the present invention, the processing unit is operable to leverage big data technology to calculate an integrity score for a registered entity by analyzing information related to the registered entity. An integrity score relates to veracity of statements made by the entity during his/her conversations with other entities, authenticity of information provided in entity profile and truthfulness of an entity during transactions on the system. The processing unit **102** is operable to analyze information related to the subject entity wherein the information is collated across chat conversations with other entities, information from one or more wearable devices connected to the system and worn by the subject entity, and information from one or more social media platforms related to the subject entity. The integrity score as calculated is associated with the entity profile. Optionally, the integrity score for a registered entity may be displayed to other entities based on the designated tier. As such, Tier-IV and Tier-III entities may be able to view an integrity score related to other entities of similar tiers which helps them to decide whether they want to continue or initiate their association with the said entity. In an example embodiment of

the present invention, an entity might state in their entity profile information as having no past relationship. However, on an analysis of their social media profiles, the processing unit can find out such edits on relationship status thereby reducing an integrity score for the said entity since the two information contradict each other. Further, using big data algorithms, multiple such data points may be cross-referenced to predict, by the processing unit 102, one or more false statements or information from the entity.

[0027] In operation, an entity registered with the system 100, places a request for connection with at least one of the other registered entities with the system **100**. In response to the said request, the processing unit is configured to access, from the database arrangement **106**, a network graph for the plurality of entities registered with the system 100. As described above, the network graph is a graph database of one or more entities and their corresponding entity profile. The entity requesting the connection to other entities is identified and tagged as the requesting node on the network graph. The processing unit then calculates an importance score, for the requesting node, in relation to other nodes of the network graph. For calculating the importance score, the processing unit employs correlation of attributes between each pair of nodes being compared wherein the attributes are retrieved from the entity profile for said nodes. The processing unit **102** is configured to identify one or more nodes with an importance score above

a predetermined threshold. In the preferred embodiment, the threshold may be set at 70% match. Alternatively, it can be further fine-tuned to any set threshold. The processing unit is further operable to display a list of said identified one or more nodes on a graphical user interface associated with a client device of the requesting node. In an embodiment, the processing unit is further operable to display, on the graphical user interface, entity profile for the identified one or more nodes.

[0028] The entity that placed a request for connection i.e. the requesting node may select one or more identified nodes on the graphical user interface and a connection request is transmitted to the said selected nodes. Such selection may be done on the basis of one or more preferred attributes, matching traits or higher integrity score. Optionally, the requesting node may not choose to send connection requests to one or more identified nodes but may provide a positive response gesture to one or more nodes. Said positive gesture response is recorded by the processing unit and is used to update the network graph. Alternatively, the requesting node may also provide a negative response gesture to one or more nodes. Said negative response gesture is recorded by the processing unit 102 and is used to update the network graph to ensure such recommendations are not shown to the requesting node in future. In effect, said negative response gestures add negative weight to the edges between the two nodes in the network graph. The processing unit **102** is further configured to communicate an acceptance

of connection request from any of the selected nodes and enables the requesting node to associate with said node through one or more interaction mediums provided by the processing unit through the graphical user interface. The one or more interaction medium includes video calls, chat messages and email communication. The network graph is further updated based on acceptance of connection requests from any of the selected nodes.

[0029] In another embodiment of the present invention, an entity may input one or more selected preferences to the processing unit via an interactive smart chat-bot. The processing unit **102** is operable to compute the importance score in relation to other entities and display the result on the graphical user interface. This method can be used by an entity to narrow down their search for a potential partner based on the most granular level of attribute and compatibility. As an example, an entity may select only the DNA and genome report to initiate association with other entities.

[0030] In yet another embodiment, the processing unit is configured to sort the one or more identified node based on the importance score and display the sorted list on the graphical user interface.

[0031] Client devices **114a1-a3** (collectively "client devices 110") are depicted as a mobile phone 110a1-a3 and a desktop computer 110b1-b3, respectively, but client devices **114** may comprise any type of computing device, such as a desktop computer system, a laptop, cellular phone, a smart

device, a mobile telephone, a tablet style computer, or any other device capable of wireless or wired communication. In some implementations, client devices **114** are configured to interact with the processing unit **102** via an application, such as a web browser or a native application, residing on the client device **114**.

[0032] In some implementations, the client devices **114** include hardware, software, or embedded logic components or a combination of two or more such components and is configured to carry out the appropriate functions implemented or supported by the client devices **114**.

[0033] In some implementations, the client devices **114** may include one or more processors, one or more memories, one or more displays, one or more interfaces, one or more components capable of inputting data, one or more components capable of outputting data, one or more components capable of communicating with any other component of the system **100** or any other component suitable for a particular purpose.

[0034] The data communication network **108** may include an ad hoc network, an intranet, an extranet, a virtual private network (VPN), a local area network (LAN), a wireless LAN (WLAN), a wide area network (WAN), a wireless WAN (WWAN), a metropolitan area network (MAN), a portion of the Internet, a portion of the Public Switched Telephone Network (PSTN), a cellular telephone network, or a combination of two or more of the foregoing.

[0035] In some implementations, the biometric server **104** may be a unitary server or may be a distributed server spanning multiple computers or multiple datacenters.

[0036] It should be noted that some of the system features described in this specification have been presented as modules or units, in order to more particularly emphasize their implementation independence. For example, a module may be implemented as a hardware circuit comprising custom very large scale integration (VLSI) circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices, graphics processing units, or the like.

[0037] A module or unit may also be at least partially implemented in software for execution by various types of processors. An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions that may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the module and achieve the stated purpose for the module. Further, modules may be stored on a computer-readable medium,

which may be, for instance, a hard disk drive, flash device, random access memory (RAM), tape, or any other such medium used to store data. Indeed, a module of executable code could be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices, and may exist, at least partially, merely as electronic signals on a system or network. Additional modules can be included without deviating from the novel art of this disclosure. In addition, each module can include any number and combination of sub-modules, and systems, implemented with any combination of hardware and/or software modules.

[0038] Method steps of the invention may be performed by one or more computer processors executing a program tangibly embodied on a computer-readable medium to perform functions of the invention by operating on input and generating output. Suitable processors include, by way of example, both general and special purpose microprocessors. The computer readable storage medium can be a tangible device that can retain and store instructions for use by an instruction execution device. The computer readable storage

medium may be, for example, but is not limited to, an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, or any suitable combination of the foregoing. A non-exhaustive list of more specific examples of the computer readable storage medium includes the following: a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk, a mechanically encoded device such as punch-cards or raised structures in a groove having instructions recorded thereon, and any suitable combination of the foregoing. A computer readable storage medium, as used herein, is not to be construed as being transitory signals per se, such as radio waves or other freely propagating electromagnetic waves, electromagnetic waves propagating through a waveguide or other transmission media (e.g., light pulses passing through a fiber-optic cable), or electrical signals transmitted through a wire.

[0039] Computer readable program instructions described herein can be downloaded to respective computing/processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper

transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing/processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing/processing device.

[0040] Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, configuration data for integrated circuitry, or either source code or object code written in any combination of one or more programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry, field-

programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, in order to perform aspects of the present invention.