

A SYSTEM FOR VERIFYING AUTHENTICITY OF USER EMAIL, AND AN APPARATUS AND A PROCESSING METHOD IN ASSOCIATION THERETO

Field Of Invention

- 5 The present disclosure generally relates to a system suitable for verifying authenticity of one or more user emails. The present disclosure further relates to one or both of an apparatus and a processing method associable to the system.

Background

- 10 In an internet/world wide web-based environment, the use of an electronic mail (email) address would be typical for the purpose of user registration (e.g., a proof that a user registering is a person and not a robot).

- Unfortunately, attempts (e.g., by fraudster(s) and/or undiligent user(s)) may be made
15 to bypass the step of providing legitimate email(s) for the purpose of the aforementioned user registration. For example, a non-existent email address could be used. Therefore, there could be attempt(s) to provide non-authentic email(s) for the purpose of user registration.

- 20 Conventionally, a test email can be communicated (i.e., to check for a response) to a provided email address to determine authenticity of the provided email address. However, communication of a test email could potentially inconvenience the user (e.g., leading to unwanted clutter in the email inbox of the user). Moreover, communication of a test email need not necessarily be a reliable form of
25 authentication (e.g., some email service providers, after receiving an email, may by default, and communicate a return signal indicative of successful connection by virtue of the fact that the test email is communicated to the domain associated with email service provider).

- 30 Other conventional techniques/solutions to determine authenticity of a provided email address includes checking whether the mailbox name is gibberish. However, such a technique could be imprecise and not robust.

Hence the present disclosure contemplates that conventional solutions/techniques do not facilitate authentication of a provided email address in a user-friendly, efficient and/or reliable manner.

- 5 The present disclosure contemplates that there is a need to improve the manner in which a provided email address can be authenticated.

Summary of the Invention

In accordance with an embodiment of the disclosure, there is provided an apparatus.

10

The apparatus can be configured to verify authenticity of at least one user email. The apparatus can be further configured to receive and process a plurality of authentic user emails. Each of the authentic user emails can be associated with a user. Each of the authentic user emails can be further associated with unique
15 identity data associated with the user of the authentic user email.

The apparatus can include a processor. In one embodiment, the processor can include a first portion and a second portion. The first portion can, for example, be coupled to the second portion. Coupling can be by manner of one or both of wired
20 coupling and wireless coupling (i.e., at least one of wired coupling and wireless coupling).

The processor can determine (e.g., by manner of mining) at least one association between an authentic user email and a user of the authentic user email, generate at
25 least one association signal based on at least one determined association and generate, based on the at least one association signal, a deep learning model which can be used to verify authenticity of at least one user email.

In one embodiment, the first portion can be configured to receive information
30 corresponding to the plurality of authentic user emails. The first portion can be further configured to mine at least one association between an authentic user email and the user of the authentic user email. The first portion can yet be further

configured to generate and communicate at least one association signal based on at least one mined association.

The second portion can be configured to receive the at least one association signal for processing in a manner so as to generate a deep learning model. The deep learning model can be used as a basis for verifying authenticity of the at least one user email.

In one embodiment, the first portion can correspond to a learning portion. Additionally, the at least one association can be mined by manner of mapping words in natural language into high-dimensional mathematical spaces in the form of vector, and obtaining association by computing similarity between two vectors. Moreover, the at least one association can, for example, correspond to at least one pattern which can be learnt.

In one embodiment, the second portion can correspond to a training portion. Additionally, the at least one association signal can be processed, for the purpose of training, based on Long Short-Term Memory (LSTM) based techniques so as to generate the deep learning model.

In one embodiment, the at least one user email which authenticity is to be verified can be distinct from the plurality of authentic user emails.

In one embodiment, the user email which authenticity is to be verified is associable with a user and the user of the user email which authenticity is to be verified is associable with user identity data. Additionally, the apparatus can be configured to communicate with at least one device which can be used by a party of interest to generate and communicate at least one input signal indicative of the user email which authenticity is to be verified and/or user identity data.

In accordance with another embodiment of the disclosure, there is provided a processing method.

The processing method can include developing a deep learning model based on a plurality of authentic user emails.

5 The processing method can further include receiving input signals indicative of at least one user email which authenticity is to be verified.

The processing method can yet further include verifying authenticity of the at least one user email based on the deep learning model.

10 Each of the authentic user emails can be associated with a user and unique identity data associated with the user of the authentic user email. At least one association between an authentic user email and the user of the authentic user email can be mined. Moreover, at least one association signal can be generated based on at least one mined association. Furthermore, the deep learning model can be developed by manner of processing the at least one association signal.

15

Brief Description of the Drawings

Embodiments of the disclosure are described hereinafter with reference to the following drawings, in which:

20 Fig. 1 shows a system which can include at least one apparatus and, optionally, at least one device, according to an embodiment of the disclosure;

Fig. 2 shows the apparatus of Fig. 1 in further detail, according to an embodiment of the disclosure;

25

Fig. 3 shows the device of Fig. 1 in further detail, according to an embodiment of the disclosure;

30 Fig. 4 shows that an example computer device which can correspond to, or be associated with, the apparatus of Fig. 1 and/or the device of Fig. 1, according to an embodiment of the disclosure;

Fig. 5 shows a processing method in association with the system of Fig. 1, according to an embodiment of the disclosure; and

Fig. 6 shows a diagram illustrating an example of modules of an apparatus which can, for example, correspond to the apparatus of Fig. 2, according to an embodiment of the disclosure.

Detailed Description

The present disclosure contemplates that properly authenticating provided user email address(es) can be important for, for example, internet-based companies as proper authentication could be the basis for subsequent activities associated with such companies (e.g., commercial type activities).

The present disclosure generally contemplates the possibility of an algorithm for verifying the authenticity of one or more provided user email addresses (hereinafter simply referred to as "user email," "user emails" and/or "user email(s)") by using deep learning technology and combining multi-dimensional information (e.g., user identity data such as name of a user and birthdate of the user).

Specifically, the present disclosure contemplates that user email can generally be associated with user identity data (e.g., any one of birthdate of the user, name of the user and initials associated with the name of the user, or any combination thereof) and authenticity of a user email can be predicted based on a combination of the provided user email address and user identity data. Specifically, one or more associations between a user email and user identity data can be mined (i.e., mined data).

Moreover, the present disclosure contemplates that one or more patterns can be associated with the mined data and such pattern(s) can be learnt based on a large data sample (e.g., based on a plurality of authenticated user emails) by using neural network-based technology. Therefore, a deep learning model with very strong compatibility can be generated/developed and can be used in a wide range of

applications. Deep learning is a branch of machine learning (e.g., an algorithm utilizing artificial neural networks as a framework to characterize and learn data).

Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “scanning”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

The present specification also discloses one or more apparatuses for performing the operation(s) of one or more methods. Such apparatus(es) may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with

programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer suitable for executing the various methods / processes described herein will appear from the description below.

5

In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and
10 implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or
15 scope of the disclosure.

Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage
20 devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an
25 apparatus that implements the steps of the preferred method.

The foregoing will be discussed in further detail with reference to Fig. 1 to Fig. 6 hereinafter.

30 Referring to Fig. 1, a system 100 is shown, according to an embodiment of the disclosure. The system 100 can be suitable for use for verifying the authenticity of at least one user email.

The system 100 can include one or more apparatuses 102 and, optionally, one or both of at least one device 104 and a communication network 106.

5 The apparatus(es) 102 can be coupled to the device(s) 104. Specifically, the apparatus(es) 102 can, for example, be coupled to the device(s) 104 via the communication network 106.

10 In one embodiment, the apparatus(es) 102 can be coupled to the communication network 106 and the device(s) 104 can be coupled to the communication network 106. Coupling can be by manner of one or both of wired coupling and wireless coupling. The apparatus(es) 102 can, in general, be configured to communicate with the device(s) 104 via the communication network 106.

15 The apparatus(es) 102 can, for example, correspond to one or more computers (e.g., laptops, desktop computers and/or electronic mobile devices having computing capabilities such as Smartphones and electronic tablets). The apparatus(es) 102 can, in one embodiment, include one or more processors (not shown) which can be configured to perform one or more processing tasks which can include one or both of pattern learning based processing task(s) (i.e., referable to as “pattern learning”) and
20 algorithm training based processing tasks (i.e., referable to as “algorithm training”). Specifically, the apparatus(es) 102 can be configured to perform the task(s) of pattern learning and/or algorithm training. The apparatus(es) 102 will be discussed later in further detail with reference to Fig. 2, according to an embodiment of the disclosure.

25

The device(s) 104 can, for example, correspond to one or more host devices (e.g., one or more computers or one or more databases). A host device can, for example, be configured to host/carry a platform configured to allow a party of interest (e.g., an owner or an administrator of an internet company) to verify one or more user emails.
30 The platform can, for example, be in the form of an online platform. In a more specific example, the platform can correspond to an online based graphics user interface (GUI) which can include one or more input portions for input, by a party of interest, in a manner so as to verify one or more user emails. For example, via the

input portions, a party of interest can generate one or more input signals which can be indicative of user email(s) to be verified and/or user identity data (i.e., at least one of user email(s) to be verified and user identity data). The input signal(s) can be communicated from the device(s) 104 and received by the apparatus(es) 102. The device(s) 104 will be discussed later in further detail with reference to Fig. 3, according to an embodiment of the disclosure.

The communication network 106 can, for example, correspond to an Internet communication network. Communication (i.e., between the apparatus(es) 102 and the device(s) 104) via the communication network 106 can be by manner of one or both of wired communication and wireless communication.

The present disclosure contemplates that, in general, many users would, for example, tend to use (i.e., an example usage pattern) identity-related information (i.e., corresponding to the aforementioned user identity data such as birthdates and/or names) when creating user emails for the purpose of convenience (e.g., ease of remembering). For example, a user may use one or both of personal name(s) and birthdate to form an email address (i.e., user email).

Based on the above noted example usage pattern, the present disclosure contemplates that, in one embodiment, the apparatus(es) 102 can be configured to carry one or more portions which can be configured to determine the authenticity of at least one user email by manner of mining (e.g., mining of the relationship between mailbox name and user identity information) and/or learning (e.g., learning association(s)/pattern(s) in relation to mined data based on the aforementioned mining). The portion(s) can be one or both of hardware based portion(s) and software based portion(s) (i.e., a portion can correspond to a hardware and/or software based portion). This will be discussed later in the context of an embodiment with reference to Fig. 2, according to an embodiment of the disclosure.

Based on one or both of the aforementioned mining and learning, verification data can be produced. Verification data can be one or both of communicated from the apparatus(es) 102 to the device(s) 104 for use in association with the

aforementioned platform and used for further processing based on the input signal(s) received by the apparatus(es) 102 (i.e., input signal(s) communicated from the device(s) 104).

5 Earlier mentioned, the apparatus(es) 102 can be configured to carry one or more portions which can be configured to determine the authenticity of at least one user email. This will now be discussed based on an embodiment, according to an embodiment of the disclosure with reference to Fig. 2 hereinafter.

10 Referring to Fig. 2, an apparatus 102 is shown in further detail in the context of an embodiment 200, according to an embodiment of the disclosure.

In the embodiment 200, the apparatus 102 can include a processor (not shown) which can carry one or both of a first portion 202 and a second portion 204.

15 Moreover, the first portion and/or the second portion 202/204 can, for example, correspond to one or more algorithms. In this regard, the apparatus 102 can, for example, be configured to carry one or more algorithms which can correspond to at least one of the first portion 202 and the second portion 204 (i.e., the first portion 202 and/or the second portion 204). The first portion 202 can be coupled to the second
20 portion 204. Coupling between the first and second portions 202/204 can, for example, be by manner of one or both of wired coupling and wireless coupling.

Furthermore, in the embodiment 200, the first portion 202 can correspond to a learning portion and the second portion 204 can correspond to a training portion.

25

The learning portion can, for example, correspond to a pattern learning portion. For example, a number (e.g., tens, hundreds, thousands or hundreds of thousands) of user emails which have been verified/confirmed (e.g., previously/in past instances verified/confirmed) to be authentic (i.e., authentic user emails) can be collected (i.e.,
30 received by the apparatus 102), and based on one or both of expert experience and word vector training based techniques (e.g., “word2vec” which generally relates to a word vector training method/technique which maps words in natural language into high-dimensional mathematical spaces in the form of vectors, thus facilitating

subsequent word similarity calculations) one or more associations can be mined. Specifically, association can be obtained by computing similarity between two vectors. The association(s) can be indicative/correspond to one or more pattern(s) which can be learnt. Additionally, one or more associations mined can be referable to as “mined association(s)”. The mined association(s) can correspond to the
5 aforementioned mined data. The learning portion can be configured to generate one or more association signal(s) based on the mined association(s). The association signal(s) (i.e., which can be associated with/correspond to/indicative of the aforementioned mined data) can be communicated from the learning portion.

10 The training portion can, for example, correspond to an algorithm training portion. For example, Long Short-Term Memory (LSTM) based techniques can be used for the purpose of training. LSTM is an artificial Recurrent Neural Network (RNN) based architecture associated with the field of deep learning. A RNN is a class of artificial
15 neural networks where connections between nodes form a directed graph along a temporal sequence. Specifically, the training portion can be configured to process the above-mentioned association(s) (i.e., mined data which can, for example, be indicative/correspond to one or more pattern(s)) based, for example, on LSTM based techniques for learning in a manner so as to generate a deep learning model 206.
20 For example, the training portion can be configured to receive the association signal(s) for further processing using, for example, LSTM based techniques in a manner so as to generate a deep learning model 206.

25 The deep learning model 206 can be one or both of hardware based and software based (i.e. hardware based and/or software based; at least one of hardware based and software based).

30 In one embodiment, the deep learning portion 206 can correspond to a hardware based portion (not shown) carrying an algorithm generated/developed based on further processing of the aforementioned association signal(s) based, for example, on LSTM based techniques.

In another embodiment, the deep learning portion 206 can correspond to a software based portion (e.g., an algorithm) generated/developed based on further processing of the aforementioned association signal(s) based, for example, on LSTM based techniques.

5

In yet another embodiment, the deep learning portion 206 can correspond to a combination of hardware based and software based portions.

10 The present contemplates that the deep learning portion 206 can, in one example, be carried by one or both of the first and second portions 202/204. In another example, the deep learning portion 206 can be carried in a third portion (not shown) which is distinct from the first and second portions 202/204.

15 The deep learning model 206 can be associated with/correspond to the aforementioned verification data.

Moreover, the deep learning model 206 can be used as basis for verifying one more user emails as will be discussed in further detail with reference to Fig. 3.

20 In view of the foregoing, it is appreciable that the present disclosure, in one embodiment, contemplates an apparatus 102 which can be configured to verify authenticity of at least one user email. The apparatus can be further configured to receive and process a plurality of authentic user emails (e.g., up to hundreds of thousands of such authentic user emails). Such authentic user emails can be known
25 from history of usage, past records, user emails from reliable sources etc. (e.g. known based on previous uses, trusted records stored in databases and/or use emails from trusted corporations/organizations) and/or user emails previously verified/confirmed to be authentic. Each of the authentic user emails can be associated with a user and unique identity data (e.g., name of the user, initials of the
30 name of the user, birthdate of the user and/or birthplace of the user) associated with the user (i.e., the user of the authentic user email).

Generally, the apparatus can include a processor which can determine (e.g., by manner of mining) at least one association between an authentic user email and a user of the authentic user email, generate at least one association signal based on at least one determined association and generate, based on the at least one association signal, a deep learning model 206 which can be used to verify authenticity of at least one user email.

The processor can, in an embodiment, include a first portion 202 which can be configured to receive information corresponding to the plurality of authentic user emails (e.g., information signal(s) indicative of/corresponding to a plurality of authentic user emails) and mine at least one association (e.g., association between the name of the user of the authentic user email and the authentic user email) between an authentic user email and the user of the authentic user email. The first portion 202 can be further configured to generate and communicate at least one association signal based on at least one mined association (i.e., corresponding to mined data).

The processor can, in an embodiment, further include a second portion 204 which can be configured to receive the at least one association signal for processing in a manner so as to generate a deep learning model 206 (i.e., associated with/corresponding to verification data) which can be used as a basis for verifying authenticity of the at least one user email (i.e., a new user email, of interest to a party of interest, which authenticity is desired/needs to be verified). Specifically, a “new user email” in this context can refer to a user email which is not included in the aforementioned plurality of authentic user emails. Therefore, the at least one user email (i.e., referable to as “at least one new user email”) can be considered to be distinct from the plurality of authentic user emails.

Referring to Fig. 3, a device 104 of the system 100 is shown in further detail, according to an embodiment of the disclosure.

Earlier mentioned, in one embodiment, the device can be configured to host/carry a platform which can be configured to host/carry a platform configured to allow a party

of interest (e.g., an owner or an administrator of an internet company) to verify one or more user emails.

As shown, the platform can, for example, be in the form of an online platform 302. In a more specific example, the platform can correspond to an online based graphics user interface (GUI) which can include one or more input portions 304 for input/inputting, by a party of interest, in a manner so as to verify one or more user emails.

For example, via the input portion(s) 304, a party of interest can generate one or more input signals which can be indicative of user email(s) to be verified and/or user identity data.

Earlier mentioned, the input signal(s) can be communicated from the device(s) 104 and received by the apparatus(es) 102.

Appreciably, a party of interest can enter an email address to be verified and one or more associated identity information. One or more input signals corresponding to the entered email address and associated identity information can be generated and communicated to the apparatus(es) 102. The received input signal(s) can be processed based on the deep learning model 206 to generate one or more probability signals. The probability signals can be communicated to the device 104 for further processing in a manner such that the party of interest can visually perceive a probability concerning authenticity of the entered email address (i.e. as to whether the entered email address is authentic). In this regard, the probability signals can be further processed (e.g., by the device 104) in a manner so as to generate one or more output graphic signals. The output graphic signal(s) can be indicative of probability of authenticity (i.e., concerning authenticity of an entered email address).

It is further appreciable that convenience can be facilitated, from the party of interest's perspective, in terms of authentication of one or more user emails. Moreover, authentication of one or more user emails can be authenticated in a

reliable manner (e.g., in view of the deep learning portion 206). In one simplistic example, a party of interest needs only to enter a user email and identity information using the online platform 302 and verification result (i.e., based on the aforementioned probability signal(s)) can be obtained.

5

Moreover, given that authentic user emails can be the basis for developing/generating (learning, training etc.) the deep learning model 206, accuracy/reliability in verifying authenticity of a new user email can be facilitated. Generally, the present disclosure contemplates that it would be more reliable to
10 develop a deep learning model 206 by manner of learning the aforementioned association(s)/pattern(s) based on (known/verified) authentic user emails as opposed to attempting to detect abnormality (e.g., checking whether a mailbox name is gibberish, as discussed earlier).

15 Additionally, it is contemplated that detection of abnormality would be tedious as there could potentially be infinite possibilities/variations/combinations (i.e., detecting abnormalities case by case could potentially be a long and endless task). Hence, the present disclosure contemplates that developing a deep learning model 206 by manner of learning the aforementioned association(s)/pattern(s) based on
20 (known/verified) authentic user emails would be more efficient.

Furthermore, the need for communication of test emails can be mitigated or at least reduced. Therefore, it is appreciable that authentication of user email(s) can possibly be carried out in one or both of a user-friendly and efficient manner.

25

To put the foregoing in general perspective, the present disclosure contemplates learning the association(s)/pattern(s) between the user email(s) and identity can be helpful in developing a deep learning model 206 for verifying authenticity of future/new user emails. Authenticity of user email(s) can be based on magnitude of
30 probability. For example, a higher percentage in probability (e.g., 75% or more) can be indicative that a user email is likely authentic whereas a lower percentage in probability (e.g., 50% or less) can be indicative that a user email is not likely authentic. Moreover, there can be many types of associations, such as initials of a

user's name being used in association with the user email, the initials combined with the birthdate of a user being used in association with the user email, the full name of a user combined with the birthdate being used in association with the user email, the full name of a user combined with the birth place of the user being used in association with the user email, and so on.

Furthermore, the present disclosure contemplates that the apparatus(es) 102 and/or the device(s) 104 can generally include one or both of at least one transceiver (for receiving and/or transmitting signal(s) etc.) and at least one processor (for processing at least one signal in a manner so as to generate another one or more signals etc.), according to an embodiment of the disclosure.

In one example, an apparatus 102 and/or a device 104 can correspond to/be associated with a computing device. This will be discussed in the context of an example computing device with reference to Fig. 4 hereinafter.

Fig. 4 shows, according to an embodiment of the disclosure, an example computing device 400, hereinafter interchangeably referred to as a computer system 400. The following description of the computing device 400 is provided by way of example only and is not intended to be limiting.

As shown in Fig 4, the example computing device 400 includes a processor 404 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 400 may also include a multi-processor system. The processor 404 is connected to a communication infrastructure 406 for communication with other components of the computing device 400. The communication infrastructure 406 may include, for example, a communications bus, cross-bar, or network.

The computing device 400 further includes a main memory 408, such as a random access memory (RAM), and a secondary memory 410. The secondary memory 410 may include, for example, a hard disk drive 412 and/or a removable storage drive 414, which may include a floppy disk drive, a magnetic tape drive, an optical disk

drive, or the like. The removable storage drive 414 reads from and/or writes to a removable storage unit 418 in a well-known manner. The removable storage unit 418 may include a floppy disk, magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 414. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 418 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

In an alternative implementation, the secondary memory 410 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 400. Such means can include, for example, a removable storage unit 422 and an interface 420. Examples of a removable storage unit 422 and interface 420 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip (such as an EPROM or PROM) and associated socket, and other removable storage units 422 and interfaces 420 which allow software and data to be transferred from the removable storage unit 422 to the computer system 400.

The computing device 400 also includes at least one communication interface 424. The communication interface 424 allows software and data to be transferred between computing device 400 and external devices via a communication path 426. In various embodiments of the disclosure, the communication interface 424 permits data to be transferred between the computing device 400 and a data communication network, such as a public data or private data communication network. The communication interface 424 may be used to exchange data between different computing devices 400 which such computing devices 400 form part an interconnected computer network. Examples of a communication interface 424 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 424 may be wired or may be wireless. Software and data transferred via the communication interface 424 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by

communication interface 424. These signals are provided to the communication interface via the communication path 426.

As shown in Fig 4, the computing device 400 further includes a display interface 402 which performs operations for rendering images to an associated display 430 and an audio interface 432 for performing operations for playing audio content via associated speaker(s) 434.

As used herein, the term "computer program product" may refer, in part, to removable storage unit 418, removable storage unit 422, a hard disk installed in hard disk drive 412, or a carrier wave carrying software over communication path 426 (wireless link or cable) to communication interface 424.

Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 400 for execution and/or processing. Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 400. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 400 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

The computer programs (also called computer program code(s)/algorithm(s)) are stored in main memory 408 and/or secondary memory 410. Computer programs can also be received via the communication interface 424. Such computer programs, when executed, enable the computing device 400 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 404 to perform features of the above-

described embodiments. Accordingly, such computer programs represent controllers of the computer system 400.

Software may be stored in a computer program product and loaded into the computing device 400 using the removable storage drive 414, the hard disk drive 412, or the interface 420. Alternatively, the computer program product may be downloaded to the computer system 400 over the communications path 426. The software, when executed by the processor 404, causes the computing device 400 to perform functions of embodiments described herein.

It is to be understood that the embodiment of Fig. 4 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 400 may be omitted. Also, in some embodiments, one or more features of the computing device 400 may be combined together. Additionally, in some embodiments, one or more features of the computing device 400 may be split into one or more component parts.

It will be appreciated that the elements illustrated in Fig. 4 function to provide means for performing the various functions and operations of the servers as described in the above embodiments.

In an implementation, a server may be generally described as a physical device comprising at least one processor and at least one memory including computer program code. The at least one memory and the computer program code are configured to, with the at least one processor, cause the physical device to perform the requisite operations.

Referring to Fig. 5, a processing method 500 in association with the system 100 is shown, according to an embodiment of the disclosure.

The processing method 500 can include any one of an input (or “inputting”) step 502, a developing (or “generating”) step 504 and an output (or “outputting”) step 506, or any combination thereof.

With regard to the input step 502, the aforementioned input signal(s) can be generated. As discussed earlier, the input signal(s) can be received by the apparatus(es) 102 for processing, according to an embodiment of the disclosure.

5 For example, the input signal(s) can be communicated from the device(s) 104 and received by the apparatus(es) 102 for processing.

With regard to the developing step 504, a deep learning model 206 can be developed/generated in a manner as discussed earlier with reference to Fig. 2,
10 according to an embodiment of the disclosure.

With regard to the output step 506, the input signal(s) can be processed based on the deep learning model 206 to generate one or more probability signals in a manner as discussed earlier with reference to Fig. 2 and/or Fig. 3, according to an
15 embodiment of the disclosure.

Generally, the present disclosure contemplates, in one embodiment, a processing method 500 which can include developing a deep learning model 206 (e.g., using the apparatus(es) 102) based on a plurality of authentic user emails, receiving input
20 signals (e.g., which can be generated and communicated using the device(s) 104) indicative of at least one user email which authenticity is to be verified, and verifying authenticity of the at least one user email based on the deep learning model 206.

Each of the authentic user emails can be associated with a user and unique identity
25 data associated with the user (e.g., birthdate of the user, name of the user, initials of the name of the user and/or birthplace of the user) of the authentic user email.

At least one association between an authentic user email and the user of the authentic user email (e.g., association between the name of the user of the authentic
30 user email and the authentic user email) can be mined. Moreover, at least one association signal is capable of being generated based on at least one mined association. Moreover, the deep learning model 206 can be developed/generated by manner of processing the at least one association signal.

Referring to Fig. 6, an example of modules of an apparatus 600 is shown according to an embodiment of the disclosure. The apparatus 600 can be an example of an embodiment of the aforementioned apparatus 102.

5

As shown, the apparatus 600 can include a development module 602 that develops a deep learning model 206 based on a plurality of authentic user emails, a retrieving module 604 that receives input signals indicative of at least one user email which authenticity is to be verified and a verification module 606 that verifies authenticity of at least one user email based on the deep learning model.

10

In one embodiment, the development module 602 can include one or both of a learning module and a training module. The learning module can, for example, correspond to the aforementioned learning portion and the training module can, for example, correspond to the aforementioned training portion. In this regard, the foregoing discussion, where appropriate, concerning the first portion 202 and/or the second portion 204 analogously applies.

15

In one embodiment, the input signal(s) can be generated by and communicated from the aforementioned device(s) 104.

20

In one embodiment, the verification module 606 can include/correspond to a deep learning model 206 which can verify authenticity of at least one user email.

Fig. 6 can, for example, be interpreted as illustrating an internal functional module and/or a structure of a verifying apparatus that verifies authenticity of at least one user email, according to an embodiment of the disclosure.

25

The solution(s)/technique(s) discussed in relation to one or more embodiments of the disclosure can be associated with one or more technical effects. For example, a non-intrusive mailbox (i.e., corresponding to the aforementioned user email(s)) verification system/algorithm/apparatus/device/method can be facilitated (e.g., communication of verification emails to confirm authenticity can be substantially

30

eliminated). Authentication of user email(s) can be facilitated in a user-friendly manner (i.e., convenient), an efficient manner and/or a reliable manner, as discussed earlier.

- 5 It should be further appreciated by the person skilled in the art that variations and combinations of features described above, not being alternatives or substitutes, may be combined to form yet further embodiments.

10 In one example, the aforementioned platform can be carried by (e.g., installed on) a personal computer (PC) of a party of interest. For example, the platform can be a software program which can be installed on the PC of a party of interest for use by the party of interest to verify authenticity of one or more user emails.

15 In another example, the present disclosure contemplates that all the users of the plurality of authentic user emails are different (e.g., all different individuals/persons), according to an embodiment of the disclosure.

20 In yet another example, the present disclosure contemplates the possibility that, in one embodiment, there could be identical users associated with a number of authentic user emails from the aforementioned plurality of authentic user emails (e.g., the same individual/person can be associated with two or more authentic user emails from the plurality of authentic user emails).

25 In yet a further example, the present disclosure contemplates, in another embodiment, the possibility that a user of a user email to be verified can be identical to the user of an authentic user email, albeit the user email to be verified being different from the authentic user email (i.e., the authentic user email can be distinct from the user email to be verified even though the user of the authentic user email is identical to the user of the user email to be verified).

30

In the foregoing manner, various embodiments of the disclosure are described for addressing at least one of the foregoing disadvantages. Such embodiments are intended to be encompassed by the following claims, and are not to be limited to

specific forms or arrangements of parts so described and it will be apparent to one skilled in the art in view of this disclosure that numerous changes and/or modification can be made, which are also intended to be encompassed by the following claims.

Claim(s)

1. An apparatus comprising:

a processor that:

determines at least one association between an authentic user email and a user of the authentic user email;

generates at least one association signal based on at least one determined association; and

generates, based on the at least one association signal, a deep learning model used to verify authenticity of at least one user email.

2. The apparatus as in claim 1,

wherein the processor comprises a first portion which corresponds to a learning portion, and

wherein the at least one association is capable of being determined by manner of mapping words in natural language into high-dimensional mathematical spaces in the form of vectors, and obtaining association by computing similarity between two vectors.

3. The apparatus as in claim 2,

wherein at least one association corresponds to at least one pattern which can be learnt.

4. The apparatus as in claim 1,

wherein the processor comprises a second portion which corresponds to a training portion, and

wherein the at least one association signal is capable of being processed, for the purpose of training, based on Long Short-Term Memory (LSTM) based techniques so as to generate the deep learning model.

5. The apparatus as in claim 1,
wherein the at least one user email which authenticity is to be verified
is distinct from the authentic user email.

5 6. The apparatus as in claim 1,
wherein the user email which authenticity is to be verified is associable
with a user and the user of the user email which authenticity is to be verified is
associable with user identity data, and

10 wherein the apparatus is communicable with at least one device, the
device being usable by a party of interest to generate and communicate at
least one input signal indicative of the user email which authenticity is to be
verified and user identity data.

7. The apparatus as in claim 1, the authentic user email being one of a plurality
15 of authentic user emails, each of the authentic user emails being associable with a
user and unique identity data associated with the user of the authentic user email.

8. A processing method comprising:

20 developing a deep learning model based on a plurality of authentic
user emails;

receiving input signals indicative of at least one user email which
authenticity is to be verified; and

verifying authenticity of the at least one user email based on the deep
learning model,

25 wherein each of the authentic user emails is associable with a user and
unique identity data associated with the user of the authentic user email,

wherein at least one association between an authentic user email and
the user of the authentic user email is capable of being mined and at least
one association signal is capable of being generated based on at least one
30 mined association, and

wherein the deep learning model is developed by manner of
processing the at least one association signal.