November 2020

Identity And Reputation Verification Via Social Vouching

N/A

Identity And Reputation Verification Via Social Vouching

ABSTRACT

Businesses, governments, and other entities verify the identity of customers in order to assess their trustworthiness and to avoid potential losses. Identity is often determined by confirming the ownership of an identifier, e.g., phone number. However, successfully determining an individual's ownership of an identifier is insufficient to assess the reputation or trustworthiness of the individual. This disclosure describes the use of social graphs to robustly determine the identity and trustworthiness of an individual via their associations with other individuals or entities. Data from individuals associated with a potential customer are utilized, with permission from respective users, for the purpose of identity verification and/or determination of trustworthiness.

KEYWORDS

- Identity verification
- Reputation verification
- Reputation management
- Credit check
- Credit rating
- Social vouching
- Social graph

BACKGROUND

The sign-up procedure for subscriptions, online purchases, credit cards, bank loans, etc., involves identity verification. Identity verification helps determine the trustworthiness of an individual but does not guarantee it. For example, businesses have a need to verify the identity of a new customer at the time of a sign-up to know if it is safe for them to conduct business with the customer. Reliably knowing the identity and trustworthiness of the customer can help a business

avoid the financial loss that arises from dealing with fraudsters, e.g., those who use stolen identities, credit cards, etc. and charge for goods or services with the intent to default.

Identity verification presently takes various forms, e.g., requesting for a government-issued photo identity such as a passport; asking questions ("in what city were you born?") the answers to which only a genuine user would know; etc. However, in the digital age where personal information can be shared at scale, relying on confidential information provided by the user to confirm their identity or assess their trustworthiness is unreliable.

For example, consider an individual trying to sign up for a service, e.g., a banking or wireless service. The service provider requests and obtains the current phone number of the individual. The phone number is evaluated to assess the likelihood that it belongs to the individual requesting service, e.g., by looking up public data to see if the phone number matches the legal name provided by the individual. Such a technique may confirm the identity of the individual but not their ownership of the phone number. A challenge in the form of an SMS or phone call that includes a secret code can be issued and ownership can be confirmed when the individual provides the secret code received via their claimed phone number. However, success in determining an individual's ownership of a number, while verifying possession of the phone number, says nothing of the reputation or trustworthiness of the individual.

DESCRIPTION

This disclosure describes robust techniques to verify the identity and trustworthiness of an individual. The individual provides an identifier (such as a phone number). The likelihood that the phone number belongs to the individual is assessed. After establishing that the individual is the owner of the identifier, the identifier is used in combination with a social graph to determine trustworthiness via the individual's associations with other individuals or entities.

User information is utilized for identity and trustworthiness verification with specific user consent, and is accessed and analyzed in compliance with applicable regulations, including use of appropriate encryption techniques. No data is accessed, analyzed, or stored without express permission from users that own the data. Users are provided with options to limit or deny such permissions to access data and/or to decline consent for social graph based verification as described herein.

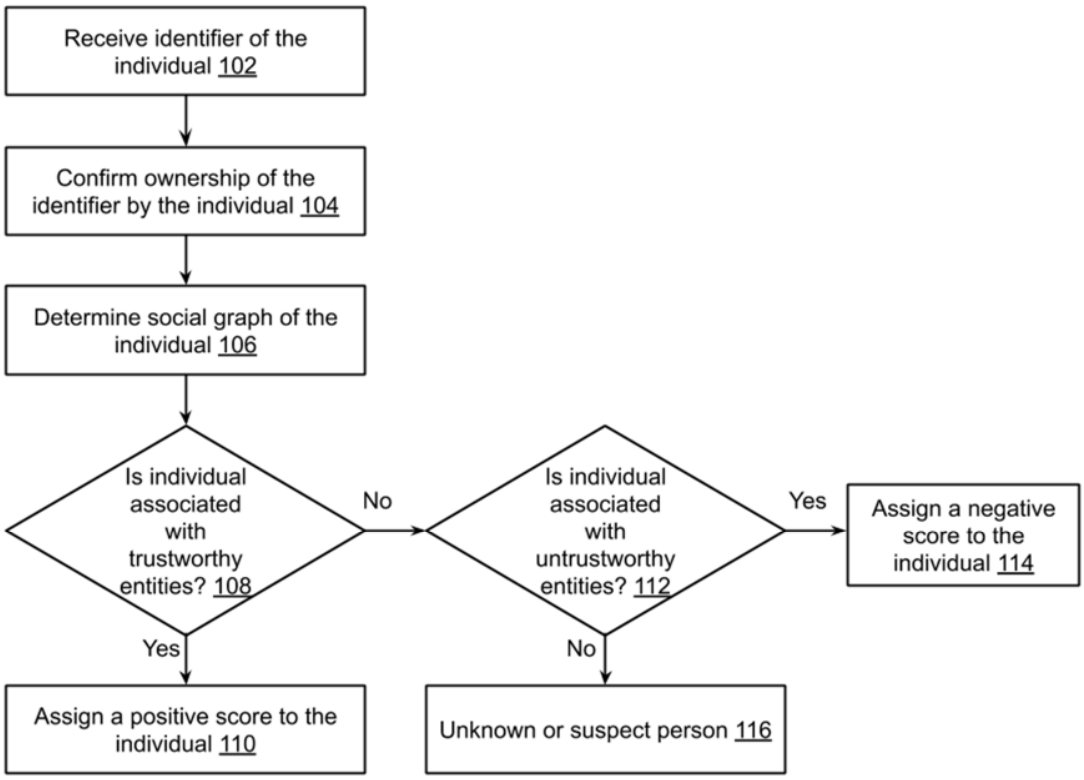

Fig. 1: Identity and reputation verification via social couching

Fig. 1 illustrates identity and reputation verification via social vouching, per the techniques of this disclosure. To establish the reputation and trustworthiness of the individual in a robust manner, an identifier, e.g., phone number, of the individual is received (102). The

ownership of the identifier is confirmed (104), e.g., by successful completion of a challenge (one-time password) by the individual.

A social graph, e.g., the links or associations between this individual and other individuals and entities of the individual, is determined (106), by accessing user-permitted data. For example, associations can be determined via public data (phone numbers listed on property records), via contact lists of other individuals, etc. If it is determined the individual is closely associated with other trustworthy individuals and entities (108), the individual is assigned a positive score (110). Else, if the individual is determined to be associated with untrustworthy entities (112), the individual is assigned a negative score (114). If the individual is not associated with other individuals or entities, the individual is determined to either be of unknown trustworthiness or be of suspect nature (e.g., bearing a synthetic or fake identity). Such an individual can be flagged for further research, and if confirmed as synthetic, can be assigned a negative score.

If an individual legitimately has few or no associations due to various circumstances, e.g., an individual that has no connections in a social graph, or if the individual is a young adult requesting service for the first time, an established individual, e.g., a guardian or other reference, can lend their score to such an individual by vouching for them. In this case, the ownership of the phone numbers of both the individual and their guardian (or reference) is confirmed, e.g., via a one-time password challenge, and the score of the guardian is substituted for the new individual. In this manner, the trustworthiness score of legitimate new individuals can be bootstrapped.

The trustworthiness score generated by the techniques can be used by a business to determine whether to do business with the individual and/or the manner in which to do business with the individual. For example, the business can proceed but place restrictions on the

individual. In the instance of a wireless service provider, data speeds granted to the individual may be throttled, or more expensive services like international roaming and long-distance phone calls may be restricted, e.g., during a probationary period.

The described techniques of using a social graph to determine the reputation of an individual is similar to techniques used by web crawlers and search engines to rank web pages in the order of quality and relevance to a given search phrase.

The described techniques for identity and reputation verification don't rely on confidential data (e.g., government-issued ID, secret questions, etc.) to identify an individual. Rather, the techniques rely on the proven ownership of an identifier and the use of the identifier to calculate a score based on data from other individuals or entities, obtained with permission for such use. The techniques are thus robust to data breaches. Also, the resulting trustworthiness score cannot be easily fabricated at scale since it is based on data from other individuals/entities. This is in contrast to techniques that use, e.g., social security numbers (SSN) or other identifiers to prove identity and trustworthiness, which may be compromised due to the availability of such data in the black market.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable the collection of user information (e.g., information about a user’s social network or social graph, identifiers such as a phone number, social actions or activities, profession, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s

geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes the use of social graphs to robustly determine the identity and trustworthiness of an individual via their associations with other individuals or entities. Data from individuals associated with a potential customer are utilized, with permission from respective users, for the purpose of identity verification and/or determination of trustworthiness.