January 2023

Secure Multi-Party Approved Information Sharing

Yen Siang Leong

Secure Multi-Party Approved Information Sharing

ABSTRACT

The technology generally relates to a plurality of users jointly and securely storing and accessing information stored in a database. The database may be a shared database in which information owners store information. Access to at least some of the information in the shared database may be granted in response to a request specifying what information is being requested. The request may be forwarded to the pertinent information owners for approval. The information owners may provide approval using multi-factor authentication (MFA). After receiving approval from the information owners, the user making the request may be granted access to the information.

BRIEF SUMMARY

This paper is generally directed to systems and methods for securely providing information stored in a shared database. The information may be provided in response to a request for information from a user. The request may include an indication of the information the user is seeking to receive, and the purpose for requesting the information. In response to receiving the request, the system may transmit a notification to the owner of the information in the shared database. An owner may approve or deny the request for information. In instances where the requested information has more than one owner, each owner may be required to approve the request before the information is provided to the user.

When approving or denying the request for information, the information owners may have to verify their identity or clearance level using multi-factor authentication (MFA). For example, to approve or deny the request, the information owners may have to use two or more authentication

factors, such as submitting a username and password, using a public and private key pair, providing a biometric authentication, submitting a username and password, completing a captcha, etc.

DESCRIPTION

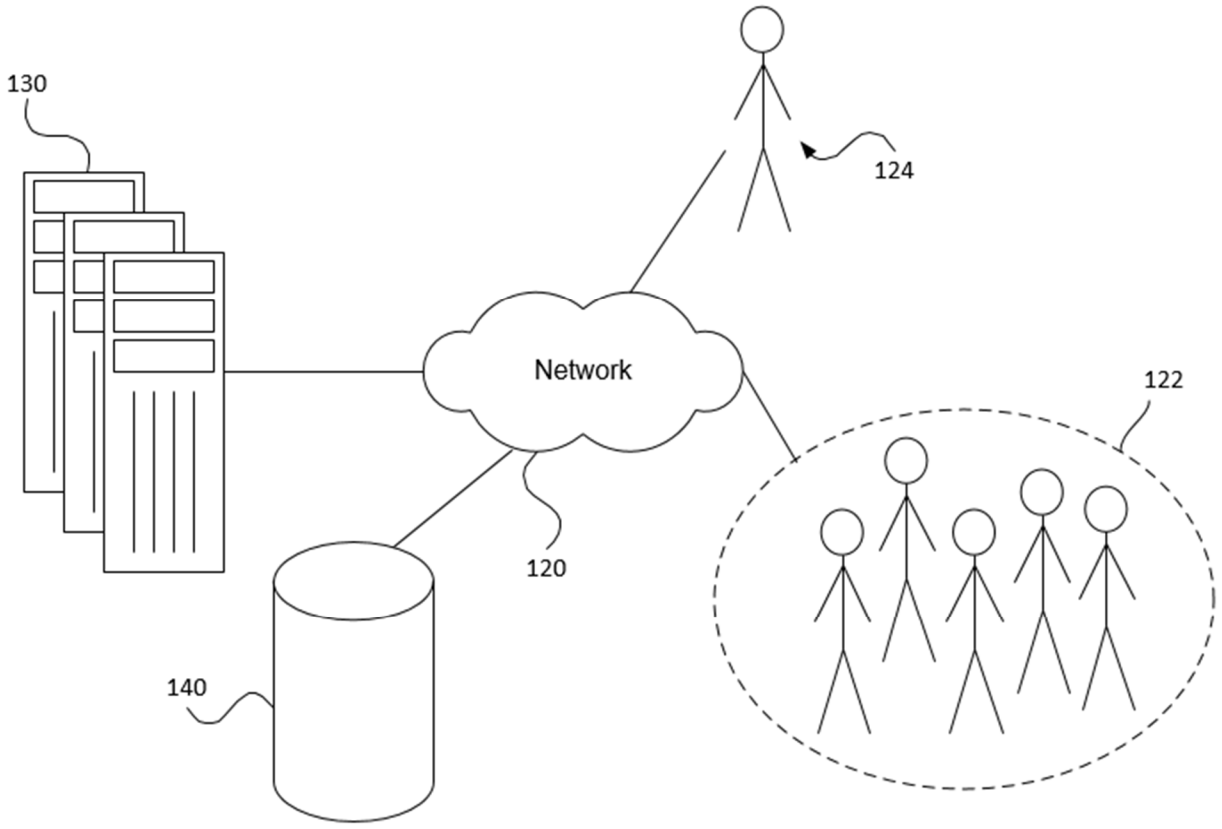

FIG. 1

Information owners 122, such as website hosts, retailers, publishers, etc., may store information in a shared database 140. The shared database may be, for example, a cloud-based database in which a plurality of users store information. The information stored in the database

may be similar. For example, the if the information owners 122 are website hosts, the information stored on the shared database may be advertisement information.

Users, who may be the information owners, may request access to the information stored on the shared database. For example, a third party user 124 that does not own information on the shared database may request access to information stored in the shared database 140. In response to the request, the server 130 that received the request may transmit an owner approval request to the information owners 122. The owner approval request may include details regarding the information request, such as who is requesting the information, the information being requested, and/or the intended use of the information. In this regard, the server 130 may require approval from the information owners 122 before the requested information can be provided to the third party user 124.

In response to receiving the owner approval request, the information owners 122 may authenticate their identity using multi-factor authentication. After authenticating their identity, the information owners 122 may approve or deny the information request by providing a response to the owner approval request back to the server 130.

The server 130 may receive the request from the third party user 124 via network 120. The request may be for information stored on shared database 140 or on the client-side of the information owners 122. For example, the shared database 140 may store information provided by the information owners 122 related to the audience or users viewing their publications, such as websites, advertisements, etc. For example, the information may be related to regarding target demographics, click conversions, optimization information, ad effectiveness, etc. The third party 124 may want to access this information to gain a better understanding of the audience viewing

certain content, the effectiveness of certain advertisements, etc. The request may be directed to information from certain information owners 122.

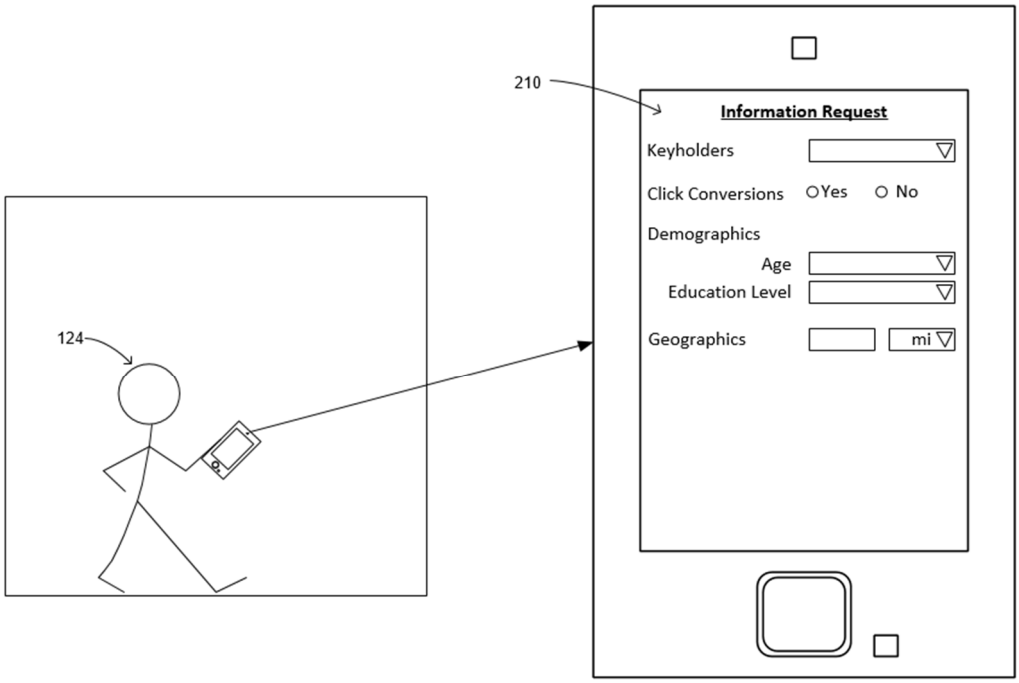

FIG. 2

As shown in Figure 2, above, the request 210 from the third party may include an indication of the information requested. For example, the request may be to receive information regarding target demographics for a particular item being offered for sale. In some examples, the request may be for click conversions for advertisements on news based websites. According to some examples, the request may include information related to the third party making the request and/or the intended use of the information received in response to the request.

In response to receiving the request for information, the system may transmit an owner approval request to the information owners 122. The owner approval request may include details regarding the request for information. The information owners 122 can either approve or deny the owner approval request. In order to approve or deny the owner approval request, the information

owners 122 may have to provide one or more authentication factors to verify that they have the credentials to approve or deny the request for information. The authentication factors may include, for example, a username and password, a public and private key pair, a biometric authentication, a username and password, a captcha, hardware authentication device, etc. According to some examples, the system may require multi-factor authentication (MFA) to approve or deny the request for information. In such an example, the information owner has to provide two or more authentication factors before being able to approve or deny the request.

The two factors of authentication may be a username and password and a hardware authentication device. The hardware authentication device may be, in some examples, a security key that can be coupled or connected to a device. As shown in Figure 3A, the first authentication factor the information owner 122 may have to provide is a username and password 350. After correctly entering the username and password, the information owner 122 may be requested to verify their authentication via a second fact. The second factor may be a hardware authentication device 352. The hardware authentication device 352 may require the information owner 122 to enter their pin 354, shown in Figure 3B, and touch the authentication device 356, shown in Figure 3C.

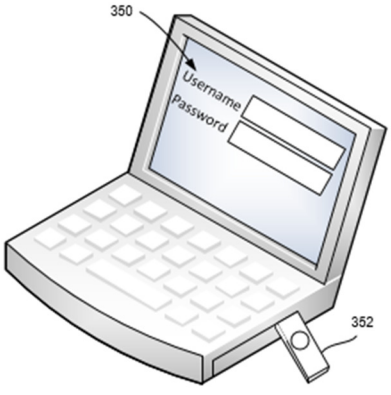

FIG. 3A

FIG. 3B

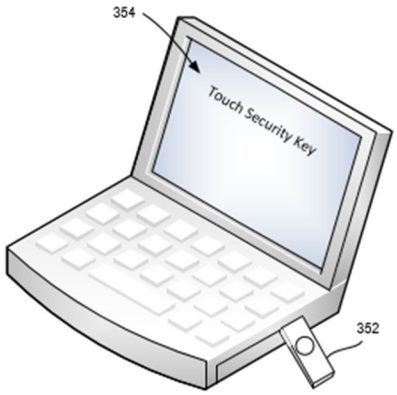

FIG. 3C

In response to receiving approval, the system may provide the requested information to the third party 124. According to some examples, the system may require approval from all information owners 122 prior to providing the information to the third party 124.