Technical Disclosure Commons

Defensive Publications Series

November 30, 2018

MECHANISM FOR TRUE OPINION SHARING

Chien Liang Lin

MECHANISM FOR TRUE OPINION SHARING

In various circumstances, people may not feel comfortable sharing opinions due to personal, cultural, or other reasons. Especially, in an organizational setting, such cultural factors may prevent members of the organization from making sound decisions at a meeting. Even with the advancement of communication technology to promote online collaboration (e.g., an email application, messaging application, among other things), anonymity may not be guaranteed. Sometimes, even if the identity of a message sender can be removed, such anonymity may not be enough for free flow of opinions if the identity of the message sender can easily be recovered. Accordingly, a mechanism is proposed for securely sharing true opinions amongst a plurality of users in the cloud storage system by an opinion sharing service.

A cloud storage system used herein refers to a system including a cloud-based environment (including a server and a data store) connected to a user device via a network. The server may host a platform (hereinafter, the platform). The platform can provide one or more applications such as an online calendar, an email, and a messenger application. Thus, users can schedule meetings for a project and communicate with each other over emails or instant messages to facilitate online collaboration via a graphical user interface (GUI) of the platform. A user or a member used herein refers to a user having a user account associated with the platform and communicating via the platform using a user device (e.g., desktop or laptop computers, mobile phones, etc.) over a network. Thus, any communication to and from a user or member described herein necessarily involves communication to the user device of the respective user or member. The GUI of the platform may be provided as a web page rendered by a web browser or a mobile or desktop application. A new feature provided by the opinion sharing service may be added to the platform as a plug-in software and may be visible on the GUI of the platform. The

data store of the cloud storage system may store data (e.g., messages and keys for encryption and decryption) resulting from communication between user devices via the platform and GUI generated for the opinion sharing device. Alternatively, the method may be performed in any system outside the cloud storage system.

The opinion sharing service may utilize group oriented cryptography to ensure secure and anonymous communication amongst a group of people (the group oriented cryptography is described in details below with respect to block 115). Specifically, the opinion sharing service may generate a public key for a group and a private key for each member of the group for encryption and decryption, respectively. The opinion sharing service may distribute the public key to all members to encrypt messages. The content of encrypted messages are to be shared among them (i.e., the members who entered the discussion forum). On the other hand, the opinion sharing service may keep the private key for each member. As such, for each encrypted message, the opinion sharing service can use a respective member's corresponding private key to decrypt the encrypted message from the respective member. The opinion sharing service can select the corresponding private key for the decryption based on, for example, a network protocol header ID information of the encrypted message as an indicator for identify of the respective member. After the decryption, the opinion sharing service can broadcast or post content of the decrypted message in a plain text form for the discussion forum. The opinion sharing service may broadcast the content of decrypted message one at a time or all at once, thereby causing presentation of such content on each member's GUI. Accordingly, the opinion sharing service can only disclose contents of messages and not identity of members who sent the messages. In this way, the opinion sharing service can promote sharing opinions while securing anonymity of the opinions.

Figure 1 illustrates a flow diagram of a method for sharing true opinions amongst a plurality of users in the cloud storage system by the opinion sharing service. First, at block 115, the opinion sharing service may, generate a group public key and a plurality of member private keys. That is, the opinion sharing service may use group oriented cryptography to enable sharing of true opinions amongst members. Group oriented cryptography is a cryptography scheme that provides secure communication among members of a group as a variation of asymmetric encryption. Asymmetric encryption involves using a key pair to secure information. A key pair is comprised of a private key (for decryption), which may be known only to a single user or a limited group of users, and a public key (for encryption), which may be known to anyone. In order to encrypt and decrypt a message, both the private key and public key are used. For example, a message will be encrypted by using the public key and transmitted to a recipient. Once the recipient receives the encrypted message, the private key is used to decrypt the message. Likewise, group oriented cryptography involves using a public key for the group (or a group public key), which may be known to members of the group and a private key (or a member private key) for each member of the group. Accordingly, the opinion sharing service may generate a group public key for the group to be distributed to members of the group and a plurality of member private keys for each member of the group. Each member private key may correspond to each member of a group. The group public key may be used to encrypt a message by a sending member. The encrypted message may be decrypted only by a member private key that corresponds to the sending member. Details about using the group public key and a member private key by the opinion sharing service for secure communication amongst the members are described below.

The opinion sharing service may generate the group public key and the plurality of member private keys, in response to receiving a request to create a group. The request may include a list of group members and may be received via the platform. For example, to send the request to create a group, a user may log into the platform and initiate the opinion sharing service by selecting an option on a home screen GUI of the platform or launching an appropriate web application available via the platform (e.g., the opinion sharing service may be provided as a plug-in software to the online calendar, email, and/or messenger application).

Once the user has initiated the opinion sharing service, the opinion sharing service may provide a GUI of the opinion sharing service that enables the user to create a group for a discussion forum. A discussion forum is a virtual space provided to users to exchange opinions via the platform. The opinion sharing service may receive the request to create a group that includes a list of members (i.e. a user profile name or user id of user accounts of the members). The opinion sharing service may identify user accounts of the members and generate member private keys for each user account associated with the platform.

Subsequently, at block 125, the opinion sharing service may, responsive to receiving from a first member a request to open a discussion forum for the group, send an invitation message to members of the group to join the discussion forum. The opinion sharing service may receive the request to open the discussion forum from the first member via the GUI of the opinion sharing service. After the first member launches the opinion sharing service, the opinion sharing service may provide the GUI with a GUI component (e.g., a button) to open a discussion forum. In response to receiving selection of the open discussion forum button, the opinion sharing service may send an invitation message to the rest of the group to join the discussion forum. The invitation message may be in a form of an email, a chat message, or a calendar invite,

among other things. The invitation message may include a date and time of the discussion forum and a GUI component (e.g., a button or a link) to join the discussion forum. As the time for the discussion forum approaches, the opinion sharing service may send a notification message to remind members to join the discussion forum.

Moreover, in response to receiving the request to open a discussion forum for the group from the first member, the opinion sharing service may provide a GUI for the discussion forum to the first member. The GUI for the discussion forum may comprise a discussion board that anonymously presents opinions from members who are attending the discussion forum. The opinion sharing service may not provide, on the discussion board, any identification (e.g., a user profile name or a user id) of members who are expressing their opinions in the discussion forum. For example, the opinion sharing service may simply present contents of messages without indicating who has sent the messages. The opinion sharing service may also provide in the discussion board an indication of a number of members who are joining the discussion forum without disclosing their identity.

Because the first member is hosting the discussion forum, the opinion sharing service may provide an additional GUI component (e.g., a button) to start discussion and to end discussion on the GUI for the discussion forum. Accordingly, until the start discussion button is selected by the first member, the opinion sharing service may not allow anybody to post a message to the discussion board. Further, in response to receiving a selection of the end discussion button by the first member, the opinion sharing service may close the discussion forum. The opinion sharing service may further provide a GUI component to initiate voting as described in details below. The opinion sharing service may also provide an invitation option to the first member to send an invitation message to one or more users of the platform to join the

discussion forum. In such case, the opinion sharing service may generate the group public key and the plurality of private keys after the first member finishes inviting all users (i.e. once members of the group for discussion forum has been set).

Subsequently, at block 135, the opinion sharing service may send the group public key to each member who joined the discussion forum. The group public key is to be used by a user device of a member to encode a message containing opinions to be posted on the discussion board. For a member to join the discussion forum, the opinion sharing service may request the member to log into the discussion forum using a user account associated with the platform once the member selects the GUI component included in the invitation message. As such, by requesting members to log into the discussion forum, the opinion sharing service may identify who has joined the discussion forum in order to send out the public group key.

Next, at block 145, responsive to receiving an encrypted message from a second member who joined the discussion forum, decrypt the encrypted message using a member private key that corresponds to the second member. After the second member joins the discussion forum, the opinion sharing service may provide to a user device of the second the GUI for the discussion forum that includes the discussion board to post opinions. When the second member sends a message including message content (i.e., an opinion) to the opinion sharing service, the user device of the second member may encrypt the message based on the group public key. The message may be encrypted using an encryption algorithm such as Rivest–Shamir–Adleman (RSA). The encrypted message may be transmitted as one or more packets, such as a Universal Datagram Protocol or Transmission Control Protocol (TCP) packets, among other things. A header of the packets may include a user identification (ID) associated with a user account of the respective member and message content (i.e. opinion being shared).

The opinion sharing service may determine which member private key to use in order to decrypt the encrypted message based on the user ID included in the encrypted message. For example, the opinion sharing service may determine that the received encrypted message is from the second member by identifying the user ID of the received encrypted message. Then the opion sharing service may use the member private key corresponding to the second member to decrypt the received encrypted message for the second member. The opinion sharing service may continue decrypting encrypted messages after receiving, from the first member, selection of the GUI component for starting the discussion and until receiving selection of the GUI component for ending the discussion.

Then, at block 155, the opinion sharing service may anonymously present the message content. For example, the opinion sharing service may post only the message content (i.e., opinion) of the decrypted message on the discussion board of the GUI for the discussion forum, without revealing who has sent the message. The opinion sharing service may update the discussion board as it receives encrypted messages and decrypted messages or all at once after receiving messages from all participating members. When posting opinions, the opinion sharing service may not indicate which member has sent which opinion. In this way, members can freely discuss their true opinions because nobody can find out who said what. That is, without the member private keys, no member can decrypt the encrypted message even if a member tries to intercept the encrypted message being sent to the opinion sharing service.

Alternatively, or in addition, the opinion sharing service may provide a mechanism for anonymous voting. The opinion sharing service may provide to members joining the discussion forum with voting option GUI components (e.g., “I agree” and “I disagree” buttons) on the GUI for the discussion forum. As for the first member (i.e., the host of the discussion forum), the

opinion sharing service may additionally provide a GUI component for voting (e.g., start voting button) on the GUI for the discussion forum. Accordingly, in response to receiving selection of the GUI component for voting from the first member, the opinion sharing service may present the voting option GUI components (e.g., “I agree” and “I disagree” buttons) on the GUI for the discussion forum for all members participating in the discussion forum. Then, the opinion sharing service may receive encrypted voting message (e.g., “I agree” or “I disagree”) from the members. The opinion sharing service may decrypt the encrypted voting message in a similar manner as described above by using appropriate member private keys. After decrypting all voting messages received, the opinion sharing service may tally voting options (e.g., “I agree” or “I disagree”) included in the voting messages. The opinion sharing service may update the discussion board on the GUI for the discussion forum to present voting results such as how many members have voted “I agree” and “I disagree”.

The opinion sharing service may additionally provide a range of voting ID to participating members, for example, from 0001 to 1000, to select a temporary ID for voting. The opinion sharing service may further ensure that every member has selected a unique voting ID. If the same voting ID has been selected by a plurality of members, the opinion sharing service may request the members who have selected the same ID to pick a different number or assign voting IDs. In case of using the voting ID, the opinion sharing service may provide the voting results indicating voting IDs associated with each voting options. For example, the opinion sharing service may present how many members have selected “I agree” option and a list of voting IDs voted for “I agree” option. In this way, all members participating in the discussion forum can confirm whether the voting result is correct.

Finally, at block 165, the opinion sharing service may, responsive to receiving a request from the first member to close the discussion forum, delete the group public key, the plurality of member private keys, and any messages received from members of the group in the discussion forum. The opinion sharing service may receive selection of the GUI component to end the discussion from the first member. Then, the opinion sharing service may close the discussion forum and delete the keys generated for encryption and decryption (i.e., the group public key and the plurality of member private keys), as well as any messages received. By deleting the plurality of member private keys, the opinion sharing service may permanently prevent any intercepted encrypted messages from being decrypted.

ABSTRACT

A mechanism is proposed for sharing true opinions amongst a plurality of users in a cloud storage system. An opinion sharing service may generate a group public key and a plurality of member private keys. Responsive to receiving from a first member a request to open a discussion forum for the group, the opinion sharing service may send an invitation message to members of the group to join the discussion forum and, for those who joined, send the group public key to each member who joined the discussion forum. Once receiving a message encrypted using the group public key from a second member, the opinion sharing service may decrypt the encrypted message using a private key that corresponds to the second member. Next, the opinion sharing service may anonymously present the message content.

Keywords: group-oriented cryptography, secure group communication, anonymous messaging, untraceable messaging, secure messaging, anonymous voting, electronic voting.

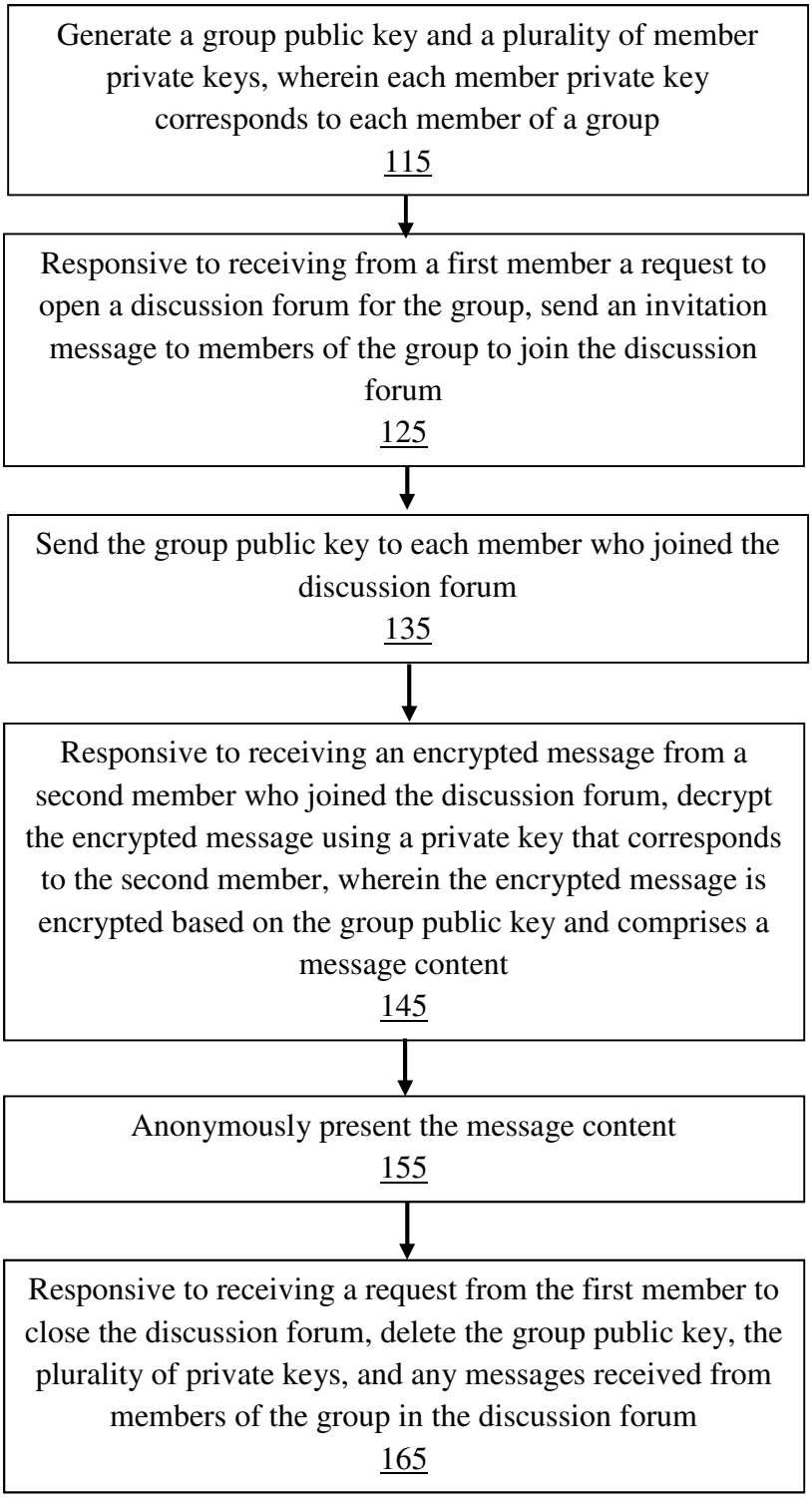
Generate a group public key and a plurality of member private keys, wherein each member private key corresponds to each member of a group
115
Responsive to receiving from a first member a request to open a discussion forum for the group, send an invitation message to members of the group to join the discussion forum
125
Send the group public key to each member who joined the discussion forum
135
Responsive to receiving an encrypted message from a second member who joined the discussion forum, decrypt the encrypted message using a private key that corresponds to the second member, wherein the encrypted message is encrypted based on the group public key and comprises a message content
145
Anonymously present the message content
155
Responsive to receiving a request from the first member to close the discussion forum, delete the group public key, the plurality of private keys, and any messages received from members of the group in the discussion forum
165

FIG. 1