Technical Disclosure Commons

Defensive Publications Series

May 01, 2017

CROSS-DEVICE PRIVATE SEARCH

Iyad Assad

Matthias Heiler

CROSS-DEVICE PRIVATE SEARCH

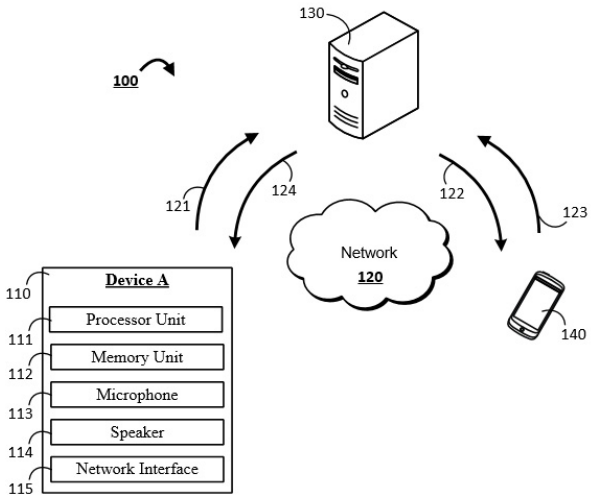
BACKGROUND

Some technologies typically provide a user with a limited number of options to access the user's stored data. For example, a user may access the user's data that is stored locally on a user device when the user is in physical proximity to the user device. Alternatively, a user may access the user's stored data through other devices if the data the user is attempting to access has been previously transmitted to, and stored on, a cloud service owned by a service provider. These limited options can force a user to choose between (i) privately storing the user's data on the user's device and not being able to search the data from a different device or (ii) entrusting a service provider with the user's data to facilitate access to the user's data across multiple devices via the cloud.

The limitations of such technologies is readily apparent with respect to a specific example. Using these technologies, a user, "Alex," may have data such as text messages, emails, pictures, or the like stored on his phone. The data stored on Alex's phone may be considered "private" because the data is stored on Alex's device as opposed to the data being stored on a third party server of a service provider. Alex can search the "private" data stored on his device such as text messages, emails, pictures, or the like when Alex is in close proximity to the device. For example, Alex can hold the phone, type in a search query, and instruct the device to search for a particular message. Alternatively, or in addition, some devices may allow Alex to perform the aforementioned search using a voice query. However, in such instances, Alex's device must still be within close proximity to Alex so that the microphone of the device can obtain data corresponding to a voice query uttered by Alex.

Alex's options for searching the data that is stored on Alex's device when the device is no longer in close proximity (e.g., the device is another room, another location, far enough away to no longer obtain data corresponding to an uttered voice query, or the like) are limited using these technologies. In such instances, for Alex to be able to access data such as text messages, emails, pictures, or the like stored on his device that is no longer in close proximity, Alex must have previously stored the data (e.g., text messages, emails, pictures) on a third-party server of a service provider. Once the data (e.g., text messages, emails, pictures) from Alex's device is uploaded to a third-party server of the service provider in the cloud, Alex may use a different device (e.g., tablet, laptop, desktop, home assistant, smart TV, car media device, or the like) to access the data stored on the third-party server of the service provider in the cloud. However, this implementation requires Alex to move his previously "private" data into the cloud. In such instances, Alex's data is no longer "private."

Figure 1 shows an example of a system 100 that facilitates cross-device private search. Cross-device private search allows a user of device A 110 to search data (e.g., text messages, emails, pictures, or the like) privately stored on device B 140 without device B 140 uploading the data (e.g., text emails, pictures, or the like) for storage in the cloud on a third-party server 130 of a service provider. An example of a system 100 that facilitates cross-device private search is provided in FIG. 1:



The device A 110 is capable of receiving user queries and generating results to the user queries. The queries received by device A 110 may be received by any mechanism including a keyboard, a mouse, a touch screen, a microphone, a speaker or a combination thereof. In some implementations, device A 110 may include a smartphone device, a tablet computer, a smartwatch, a laptop computer, a desktop computer, a media device, or the like. Alternatively, the device A 110 may include a home assistant device that is configured to detect voice queries, perform operations in response to the detected voice queries, output data that is responsive to the voice query, and the like. The device A 110 may be in close proximity to the user. For example, the device A 110 may be held in the user's hand, in the same room as the user, within a sufficient range such that the microphone 116 of the device A 110 is capable of detecting voice queries from the user, or the like.

The device B 140 may include any appropriate device that is capable to storing user content. For example, the device B 140 may include a smartphone device, a tablet computer, a smartwatch, a laptop computer, a desktop computer, a media device, a network storage device, or the like. The device B 140 may include data storage that allows for the local storage of data such

as text messages, emails, pictures, or the like. The memory unit 114 may include RAM, flash memory, disc storage, a combination thereof, or the like. The device B 140 can store data (e.g., text messages, emails, pictures, or the like) locally in device B's 140 storage unit, search locally stored data in device B's 140 memory unit, and retrieve locally stored data from device B's 140 storage unity. The device B 140 may be in close proximity to the user (e.g., in the user's hand, in the same room, within the range of device B's 140 microphone, or the like). Alternatively, the device B 140 may not be in close proximity to the user (e.g., in another room, outside of the range of device B's microphone, in a different building, in a different neighborhood, or the like).

Device A 110 and device B 140 may be linked using an authentication mechanism. For example, in some implementations, the device A 110 and device B 140 may be linked to the same account using the authentication mechanism.

The device A 110 may receive a request for content such as a voice query. In some implementations, the device A 110 may use an application stored in the memory unit 112 to determine, based on the (i) one or more parameters of the request, (ii) based on the context of the request, (iii) based on a history of requests made by the user, or (iii) a combination thereof, the location of data that is responsive to the query. For example, the device A 110 may determine whether the request for content is a request for content that is stored on the device A 110, a request for content stored on the device B 140, a request for content stored on a device that is different than device A 110 and device B 140, or the like. In some implementations, the determination of the location of the data may be based on an express instruction from a user. For example, the location of the data may be determined to be on device B 140 based on the voice query "what did Steve's email stored on device B say?" In other implementations, the determination of the location of the data may be based on an implied instruction. For example,

the user previously requested text messages from Steve from device B 140. Then, when the user subsequently submits a request for text messages from Steve, device A 110 may determine that the request is likely for text messages from device B 140 since the user previously requested text messages from device B 140, the user stores all of the user's text messages on device B 140, or the like. In a similar manner, device A 110 may determine that the requested data is not on one or more particular devices based on the received request.

After receiving the request for data, the device A may determine, based on the location of the requested data, whether the search should be executed locally on device A or whether the requested data needs to be obtained from a remote device such as device B 140. In response to determining that the search should be executed locally, the device A may execute the search and return a set of search results responsive to the search. Alternatively, or in addition, if device A 110 determines that some, or all, of the data should be retrieved from a remote device B 140, then the device A 110 can transmit 121 the request for data to device B 140 indirectly via network 120 using a secure channel connection to remote server 130 of a service provider. In such instances, the transmitted request for data may be encrypted using private-key encryption techniques, where the private keys are kept locally on device A 110 and device B 140, respectively, and never transmitted through the service provider.

The server 130 can receive the transmitted request for data, and access a user account profile associated with device A 110. The server 130 can then determine a remote device where the received request for data should be transmitted. The remote device may be selected based on the received request for data, the user account profile, or both. The server can then forward 122 the received request for data to the determined remote device such as device B 140. The device B 140 can receive the forwarded request for data and can decide to process the received request

for data, or not, based on permissions defined by the user of device B. The device B may use a private key to decrypt the request for content, execute a search query based on the request for content, and generate a set of search results responsive to the request for content. The set of search results responsive to the request for content may be encrypted, and then transmitted 123 through a secure channel established between server 130 and device B 140.

The server 130 can receive the transmitted set of search results, and access a user account profile associated with device B 140. In some implementations, the server 130 may supplement the received search results with Internet search results obtained using a search engine. The Internet search results may be identified based on the initial query received by server 130 from device A 110. The server 130 can then determine where the received set of search results should be forwarded. The destination where the received set of search results should be transmitted may be based on the received set of search results, the user account profile, data associated with an established session between the device A, the server 130, and the device B 140. In some implementations, the server 130 may determine that the search results should be forwarded 124 to the device A. The device A may output the received search results by displaying the search results on a screen associated with the device A, outputting the search results as an audio output using the speaker 114, or a combination thereof.

By way of example, a user Alex may utter a voice query that is detected by a home assistant device. For example, Alex may utter a voice query such as “what did Iyad reply on Whatsapp.” The home assistant may detect the query, and forward the query request to one or more service provider servers. Applications operating on the server may be linked to other devices for Alex and determine that Alex enabled the search across device feature. The service provider server may forward the search request to the one or more other devices along with the

public key for the user's home assistant device. Alex's phone receives the request, finds the message, may convert the message to a voice reply (or send it as text), encrypts the data with the public key for the home assistant, and sends the results to the one or more service provider servers. Then, the service provider server may forward the results to the home assistant device, and the home assistant device may output the search results. In one implementations, the home assistant device may convert one or more of the search results from text to speech, and output the one or more search results using a speaker of the device.

Alternatively, in other implementations, the device A 110 and the device B 140 may directly communicate with each other via the network 120. For example, in some implementations, device A 110 and device B 140 may be located in close proximity to one another. Accordingly, in such instances, device A 110 may communicate directly with device B 140 using a direct connection established via WiFi, Bluetooth, or the like without the need to exchange messages including search queries, search results, and the like with a service provider server.

ABSTRACT

A system is described that facilitates cross-device private search. The cross-device private search may facilitate using a first device to search content on a second remote device without the second remote device uploading the content to a cloud server. A query received on the first device may be forwarded to a third-party server of a service provider. Then the service provider can forward the query to the second remote device, receive search results from the second remote device based on the query, and forward the search results to the first device. Alternatively, in some implementations where the first device and second device are in close proximity, the first device and the second device may directly communicate with each other without the need to exchange communications via the service provider server.