January 2021

User Authentication to Provide a Secure Cloud Clipboard

Brett Aladdin Barros

Alexander James Faaborg

User Authentication to Provide a Secure Cloud Clipboard

ABSTRACT

Cloud clipboards that allow seamless copy-pasting of content across devices associated with the same user account are available. However, at present, such clipboards provide content on all devices that are logged in to the user account, which can cause inadvertent leakage of information of the clipboard to another person that may be using a user device at the time the information is placed on the cloud clipboard. Alternatively, the user may be offered an option to select a particular device to which the content is provided, which can fail if the user doesn't recognize the target device by name. This disclosure describes techniques to securely transfer text from a real world object to a user device. Per the techniques, prior to providing clipboard content on a target device, confirmation is obtained that the user is actively using the target device. Such confirmation can be obtained by authenticating the user, e.g., via facial recognition, or other suitable user-permitted techniques.

KEYWORDS

- Cloud clipboard
- Cloud copy-paste
- Face recognition
- Face-based unlock
- User authentication
- User presence

BACKGROUND

Cloud clipboards that allow seamless copy-pasting of content across devices associated with the same user account are available. However, at present, such clipboards provide content on all devices that are logged in to the user account, which can cause inadvertent leakage of information of the clipboard to another person that may be using a user device at the time the information is placed on the cloud clipboard. Alternatively, the user may be offered an option to

select a particular device to which the content is provided, which can fail if the user doesn't recognize the target device by name.

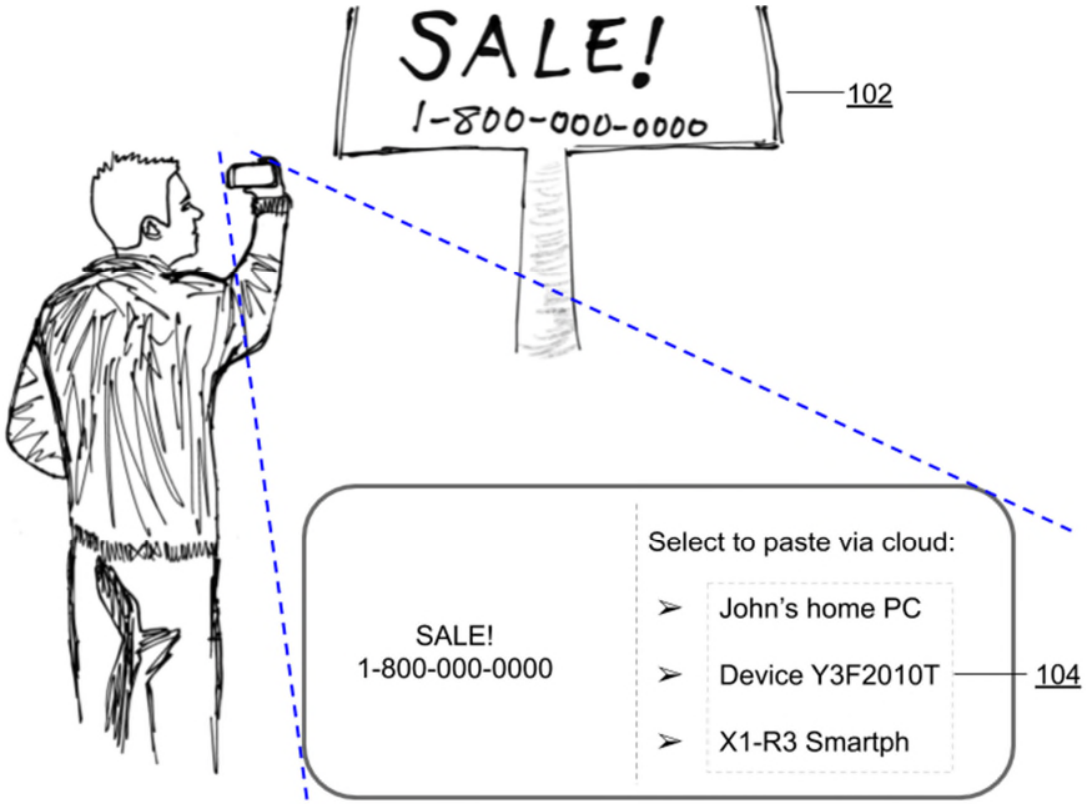

Fig. 1: Cloud-based copy-pasting

Fig. 1 illustrates cloud-based copy-pasting, which enables a user to aim a camera at any object that includes text (typed or hand-written) (102), capture an image of the object, automatically extract the text from the image, and paste the text, e.g., to send it to another device owned by the user. Prior to pasting, the user is presented with a list of devices (104) that their account is actively logged on to. This enables the user to paste the text (or other clipboard content) only to device(s) that the user authorizes. The step of offering a list of devices to paste the text on ensures that no accidental disclosure of information occurs since the clipboard content is not automatically provided to the clipboard of every device logged in with the user account, which prevents people other than the user who are using such devices access to such content.

However, offering a list of devices introduces complexity in the user interface, especially since device names are often randomly generated by the operating system or assigned by a corporate IT department, and in many cases users do not know the names of their various devices. The names of mobile devices can be particularly impenetrable, as they often include device model numbers that the user may not be aware of, e.g., A3B-2010T.

DESCRIPTION

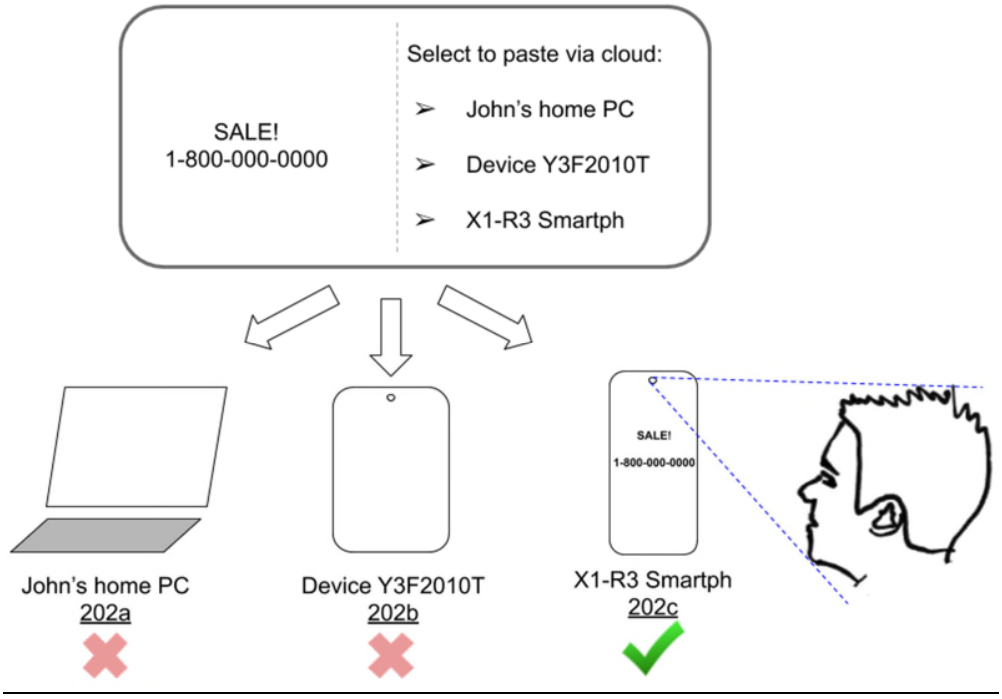

Fig. 2: Secure cloud-based copy-pasting across devices

Fig. 2 illustrates secure cloud-based copy-and-paste across devices, per the techniques of this disclosure. When a user copies text from the real world to the cloud clipboard (e.g., by obtaining it using a device camera and using optical character recognition), the text may be sent to devices (202a-c) associated with the user's account.

Per techniques described herein, a device receiving text places the text onto the local clipboard only after confirming that the user is actively using the device, and that it is not being

used by someone else. For example, such confirmation can utilize facial recognition or other suitable authentication techniques. The confirmation operation can be performed as a background process. In the example of Fig. 2, device X1-R3 Smartph (202c) is able to confirm active usage by the user using face recognition, and hence places the received text onto its clipboard. The other devices (202a-b), unable to confirm active usage by the user, do not place their received text onto the local clipboard.

While Fig. 2 shows creation of cloud-clipboard text via visual image capture, other types of content (e.g., images) as well as mechanisms of obtaining clipboard content (e.g., via a sensor other than a camera) can also be utilized to obtain content for copy-pasting. The described techniques can be implemented on any device that can extract text from real-world objects using a device camera, e.g., smartphones, wearable devices, or other devices. The techniques can be implemented as part of the device operating system, as part of a virtual assistant, or other suitable application.

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 collection of user information (e.g., information about a user's images, a user's clipboard, devices associated with a user account, 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 techniques to securely transfer text from a real world object to a user device. Per the techniques, prior to providing clipboard content on a target device, confirmation is obtained that the user is actively using the target device. Such confirmation can be obtained by authenticating the user, e.g., via facial recognition, or other suitable user-permitted techniques.