Cloud Replication for a Fingerprint Verification System

Chalee Vorakulpipat*, , Soontorn Sirapaisan*, Ekekachan Rattanaleadnusorn*, Visut Savangsuk*, Thepparit Banditwattanawong**

**National Electronics and Computer Technology Center, Thailand*
***Sripatum University, Bangkok, Thailand*

Introduction

To identify biometric data, for example, fingerprint, face and voice, a biometric verification system has been widely adopted. This is because such biometric data are considered as one of the most accurate security system nowadays [1]. However, big data of the biometric data are usually stored centralized, and are requested by clients through two-tier, three-tier, distributed systems which consume a lot of bandwidth. Therefore, using a portable mobile-based (smartphone or tablet) biometric verification system in a rural area where the internet connection is limited, such as mountainous sites are problematic when dealing with data sets. This study presents a design of a fingerprint verification system using a client-side cloud replication approach. This approach is aimed to reduce public cloud data-out expenses by using a hybrid method- offline and online, improve cloud network scalability and lower cloud service access latencies, as confirmed in another hybrid cloud approach, namely i-Cloud [2]. The adoption of this approach can enable the system in a hybrid situation, offline and online context. The proposed system is expected to let users collect and verify fingerprint data within the mobile device without internet connection.

Methods

The system architecture is divided into two parts, server and client. In the first part, a centralized public cloud server stores fingerprint data in a database management system. In the section part, a client is a mobile device which includes a fingerprint verification app and client-side cloud replica. Figure 1 illustrates the overview of proposed scheme. First, before collecting and verifying fingerprint data at mountainous sites, a user determines which villages will be chosen to collect the data at the sites. Then, the user downloads only the fingerprint data of the selected villages and stores them as replicated data in the mobile device. Once, the user moves to the villages, the user is able to collect and verify fingerprint data from local people through the fingerprint verification app and the client-side replicated data without the internet connection. Finally, when the user finishes the job and goes back to the office, the user can upload the updated fingerprint data back to the centralized cloud server to maintain eventual consistency of the replication.

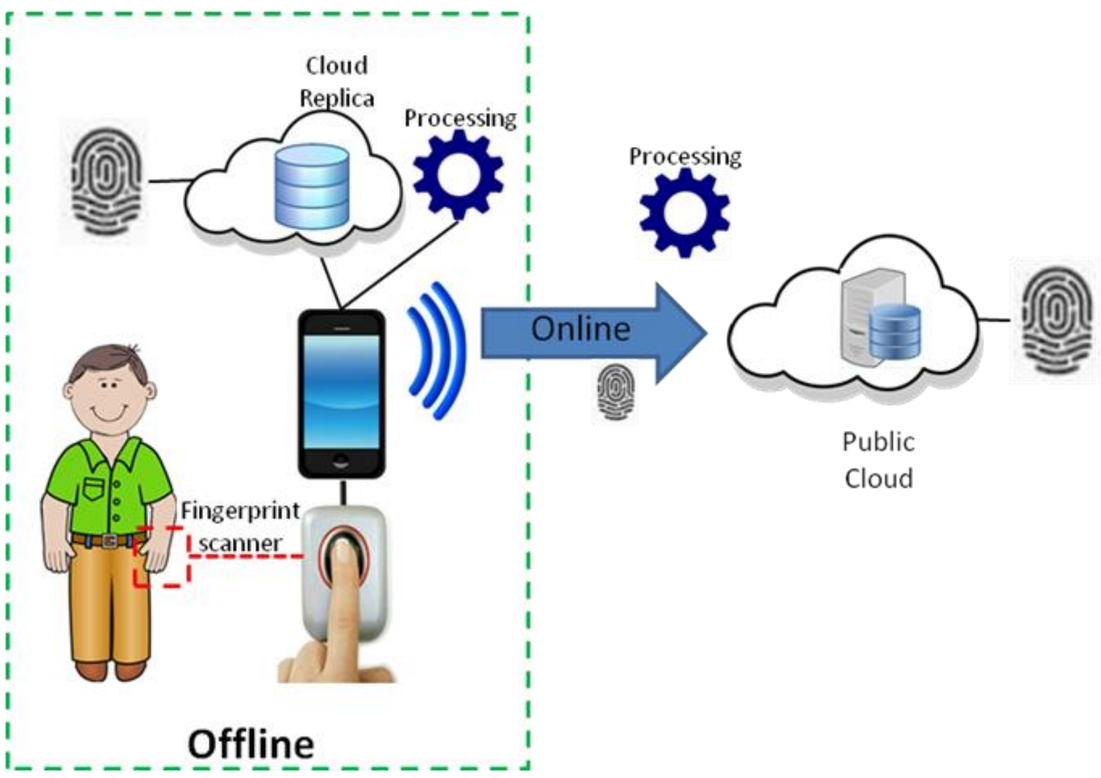

Fig. 1. Fingerprint verification system

This approach also offers a hybrid approach. During collecting data offline, once the internet is available, the mobile device can switch to an online mode to connect to the public cloud server real time. This cloud replication method can be used along with several mobile devices. Each mobile device has a unique key to deal with specific data in the public cloud. For example, mobile device 1 is used to collect fingerprint data in Village A. Only data of fingerprint of people in Village A are replicated between the public cloud server and mobile device 1. While mobile device 2 is for Village 2, only data of Village 2 will be used for replication. The conceptual framework of this cloud replication is depicted in Figure 2.

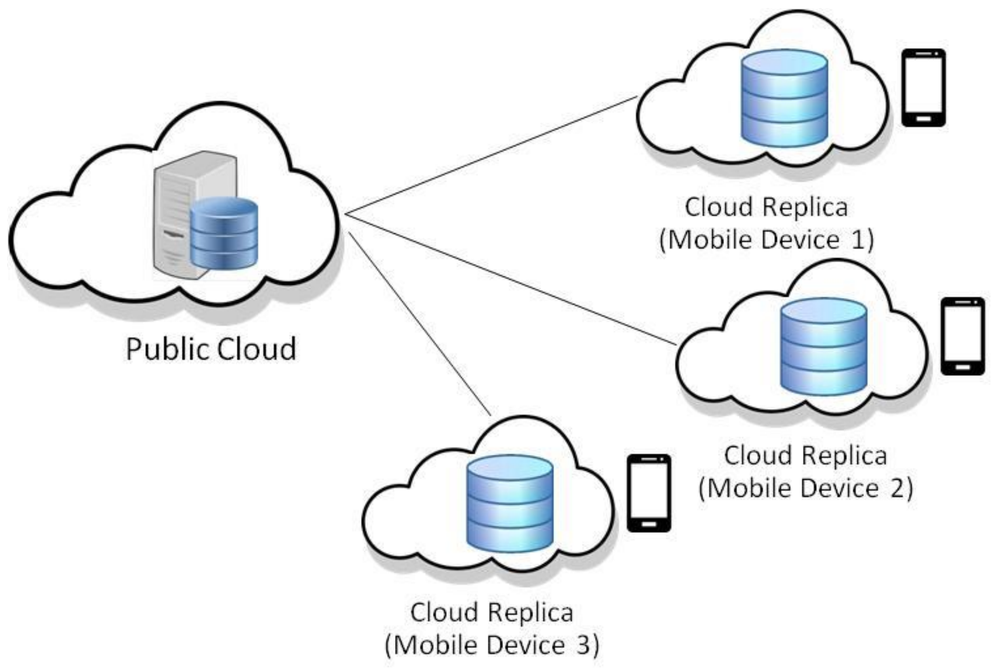

Fig. 2. Conceptual framework of cloud replication

The system using our approach was developed and evaluated by simulation, compared to the traditional client/server method. The scenarios are described as follows. Alice collected fingerprint biometrics data from local people in a mountainous village where the population was about 100 and the internet was not available. She had to complete the data collection within one trip. If she used our approach, she had to download all 100 data from the public cloud to her client before the trip. During the trip, she collected and verified data offline. After the trip, she uploaded the updated data back to the public cloud server. Fingerprint data size is about 100 kilobytes per finger (per person).

Results

Based on the scenario above, the results are simulated based on our approach and compared to a traditional client-server method of fingerprint verification. The experiment is based on the internet speed of 10 Mbps. Initial packages (i) when downloading and uploading are 300 KB. Connecting times (c) are 1 second. In Table 1, the results show that data size transferred over the internet in our approach is less than the size in the traditional method. This is because the number of connection times is only two times, while in the traditional method, the user needs to connect to the internet every time when collecting and verifying fingerprint data, thus the initial package data size in our approach are fewer. Time used for data transfer in our approach is less than time in the traditional method. This is because the number of connection times is less (only two times as mentioned above), thus the total connecting time is also less.

Table 1. The comparison of size and time between our approach and traditional method.

Method	Size	Time
Our approach	2i+20M	2c+16.32
Traditional client/server method	200i+20M	200c+16.32

Conclusions

To sum up, the client side cloud replication approach adopted for a fingerprint verification system could reduce a number of times of internet connection, resulting in increases of data size transferred over the internet and time used to transfer the data. Also, this could deliver stable performances and availability of the overall system. The system can work itself within its client side without the internet connection. This proposed client-side cloud replication approach can also be applied to other biometric e.g. face recognition or multi-factor verification and authentication system which deals with big data.

Bibliography

1. **Chien Le, "A Survey of Biometrics Security Systems", http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/, 2011.**
2. **Thepparit Banditwattanawong, Masawee Masdisornchote, Putchong Uthayopas, "Multi-provider cloud computing network infrastructure optimization", Future Generation Comp. Syst. 2016;55;116-128.**