PART 09 Personal Data Cloud

• Rahul Basava, Graduate Student
• Alex Bonomo, Undergrad
• Jeff Burke, Faculty, PI*
• Deborah Estrin, Faculty, PI
• Derek Kulinski, Graduate Student*

* Primary Contact

Overview
The Personal Data Cloud is conceptually based on the Personal Data vault project. A Personal data Vault (PDV) is a secure repository of data. The Personal Data Cloud (PDC) refers to all PDV instances controlled by a single user. The PDV instances collect, store and distribute user's data. The user can apply access controls, filters and other data altering operations before letting a particular PDV instance transfer information to another PDV instance. All the communicating PDV instances are tailored for a particular application and have the ability to understand and work with the data exchanged between them. This project deals with the design and implementation for such a PDV which can securely store and transfer data to other PDVs over the Named Data Networking (NDN).

Objectives
- User managed secure repositories for time and location traces controlled by the person whose traces they are.
- Granular and configurable sharing with provision for archiving data.
- Audit trail enforcement and API Controlled access by user authorized third-party services.
- Migration from provider to provider over lifetime.
- Deploy the project to run over the NDN network to use the security and delivery efficiencies which are built in features provided by NDN.

Technical Challenges
- Support efficient federation of queries across PDVs.
- Defining “auditing” and designing enforcement mechanisms.
- Virtualization to isolate user vaults and application data processing in cloud providers.
- Design Security and Privilege model in context of medical and legal frameworks.
- Limits circumstances for legal discovery.
- Creating standards for best practices and auditing.
- Enable a marketplace of ‘certified’ applications that adhere to the standards.

Approach
Every entity like a user’s phone or desktop is considered to be a PDV. Such PDVs will be primarily considered as sources of information generated for a particular user. The users also lease or own PDVs that may be maintained by trusted organization (Providers).

Implementation is planned for two versions for the PDC, one for the cloud based providers and the other for mobile devices developed on the android operating system. These versions will share many common security and
transmission components built on top of NDN. The two versions will differ in their ability to process information and data storage function. Also the cloud version is expected to have a very comprehensive user interface for managing data. Other function like archiving, processing and filtering will be provided to each version based on the need of specific application.

The Andwellness project is the first application that will be using the PDV framework. The Android app of Andwellness will be changed to work with the android PDC version and the server will have a proxy application that will form a intermediary between the Andwellness server and the NDN transmission system. A Cloud PDC will be developed to apply filter and restrict information sent to the Andwellness servers. The filters will initially work based on time and location information.

System Description and a Use case
The PDV instance that is sending data is called a ‘Publisher’ (PUBLISHER) and the PDV instance receiving the data is called a ‘Receiver’ (RECEIVER). A PDV instance can be both a publisher and a receiver. For example a PDV instance on a mobile phone can send data. Whereas a PDV instance in the cloud (say an instance managed by a PDV provider) could receive data from a mobile phone and in turn send data to another PDV instance after processing the data.

Since this implementation is deployed to work over the NDN, the communication is by nature connectionless and individual data records are transmitted independently from PUBLISHER to RECEIVER. The communication is inherently disruption tolerant and secure.

Transferring from Mobile phone to Personal Cloud- A use case
This use case describes how a user interacts with the PDV instances when sending data from a mobile phone (PUBLISHER) to a secure repository (RECEIVER) in the cloud managed by a PDV Provider.

1. The user downloads the Mobile application from a site whose identity is vouched for by some certificate authority like Verisign. The application gathers data about the user. This application runs a lightweight PDV instance to provide caching and disruption tolerance. The instance may also act as a store to facilitate local processing.

2. The cloud PDV instance has a user interface (UI) which allows the user to register and provides necessary information for connecting and gathering information from the applications that the user owns.

3. The user can have multiple identities based on public keys, digital signatures or username password pairs.

4. The user selects “Send Data” in the mobile application. The mobile application asks for data destination URL. The user provides the URL of the cloud PDV instance to which it has to connect for transferring data. The URL can be generated by the cloud PDV and shown to the user in the cloud PDV instance UI.

5. The mobile PDV instance initiates a stream creation process. The user types in the random token (generated by the cloud PDV) to authenticate with the cloud PDV instance. The instances automatically exchange stream related information which includes, name of the stream, key for encryption and key for signing.

6. The cloud PDV instance issues regular interests to the new stream and pulls data to its persistent store.

Progress
The implementation is in the initial stage and we are exploring the available package of NDN. The security model for transmission and the transmission mechanisms have been finalized. The Andwellness Framework (version 2.0) is in the process of being changed to work with the Mobile version of the PDC.

Future Directions
Developing the prototype implementation of the PDC for Andwellness framework is the main target. This will be followed by doing a survey for Sleep study using the new platform. The implementation will have a android PDV and a cloud based PDV with provision for time and location based filters which are user configurable.

The PDC will be extended to implement other applications.