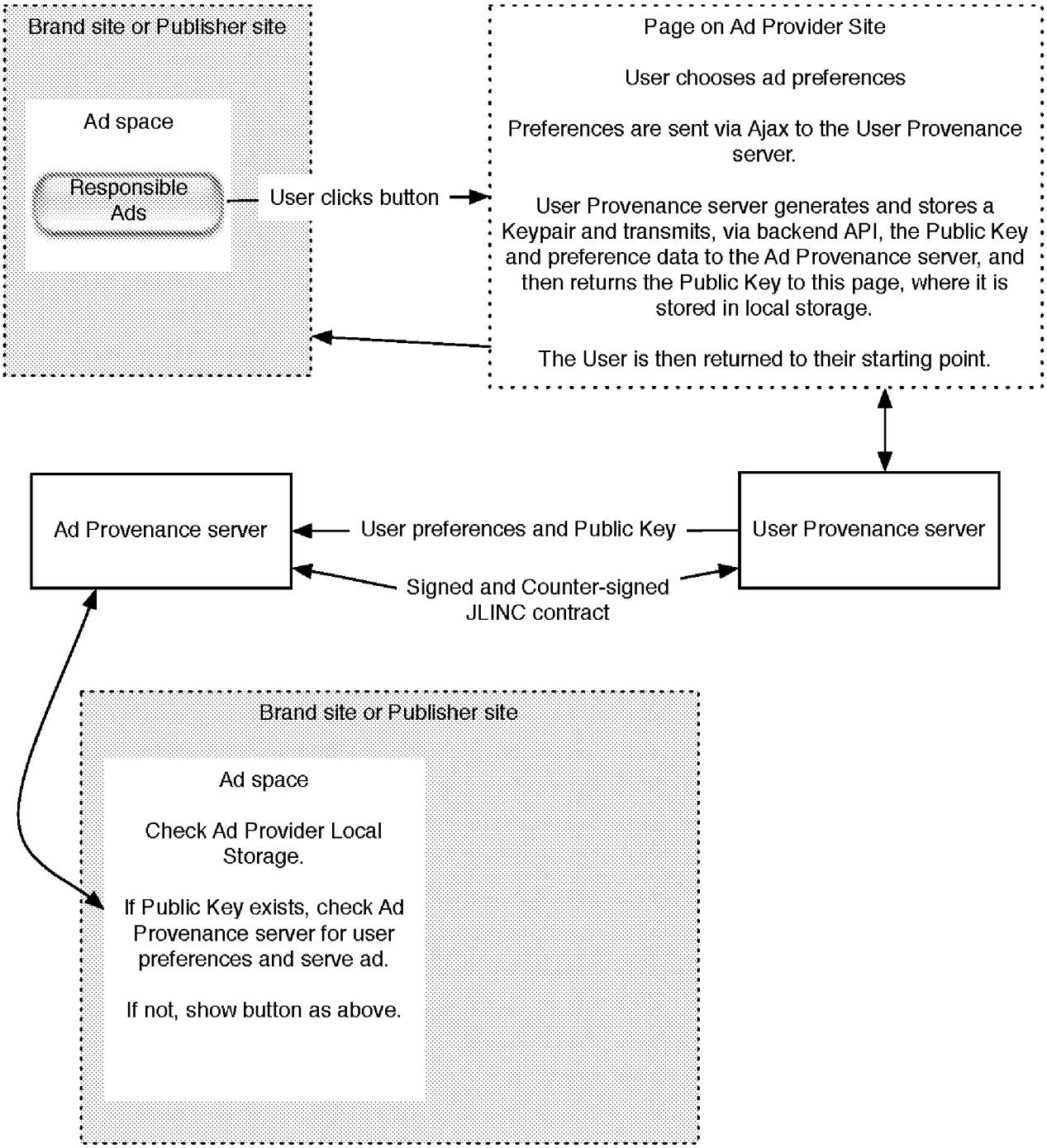

Brand site or Publisher site
Ad space
Responsible Ads
User clicks button
Page on Ad Provider Site
User chooses ad preferences
Preferences are sent via Ajax to the User Provenance server.
User Provenance server generates and stores a Keypair and transmits, via backend API, the Public Key and preference data to the Ad Provenance server, and then returns the Public Key to this page, where it is stored in local storage.
The User is then returned to their starting point.
Ad Provenance server
User preferences and Public Key
User Provenance server
Signed and Counter-signed JLINC contract
Brand site or Publisher site
Ad space
Check Ad Provider Local Storage.
If Public Key exists, check Ad Provenance server for user preferences and serve ad.
If not, show button as above.

FIG. 1

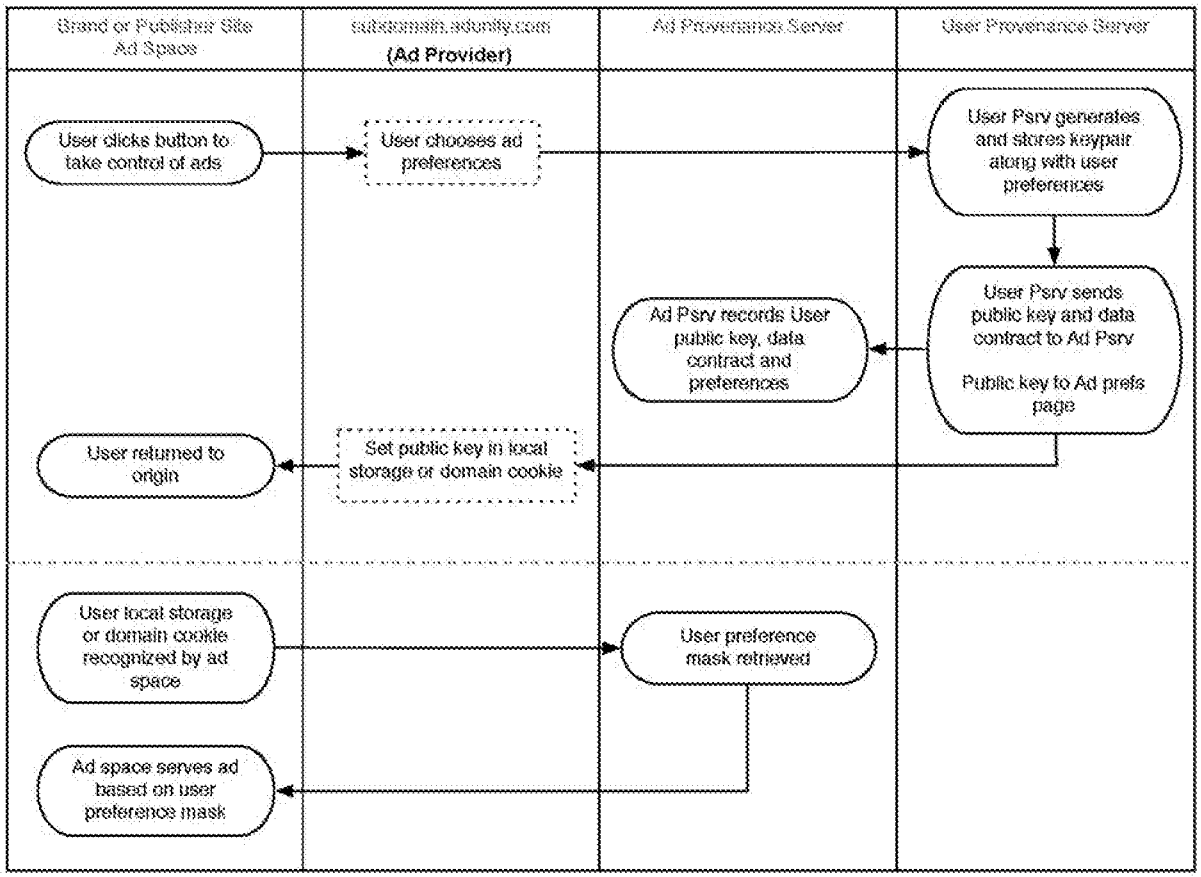

Brand or Publisher Site Ad Space
subdomain.adunify.com (Ad Provider)
Ad Provenance Server
User Provenance Server
User clicks button to take control of ads
User chooses ad preferences
User Psrv generates and stores keypair along with user preferences
User Psrv sends public key and data contract to Ad Psrv
Public key to Ad prefs page
Ad Psrv records User public key, data contract and preferences
User returned to origin
Set public key in local storage or domain cookie
User local storage or domain cookie recognized by ad space
User preference mask retrieved
Ad space serves ad based on user preference mask

FIG. 2

FIG. 3

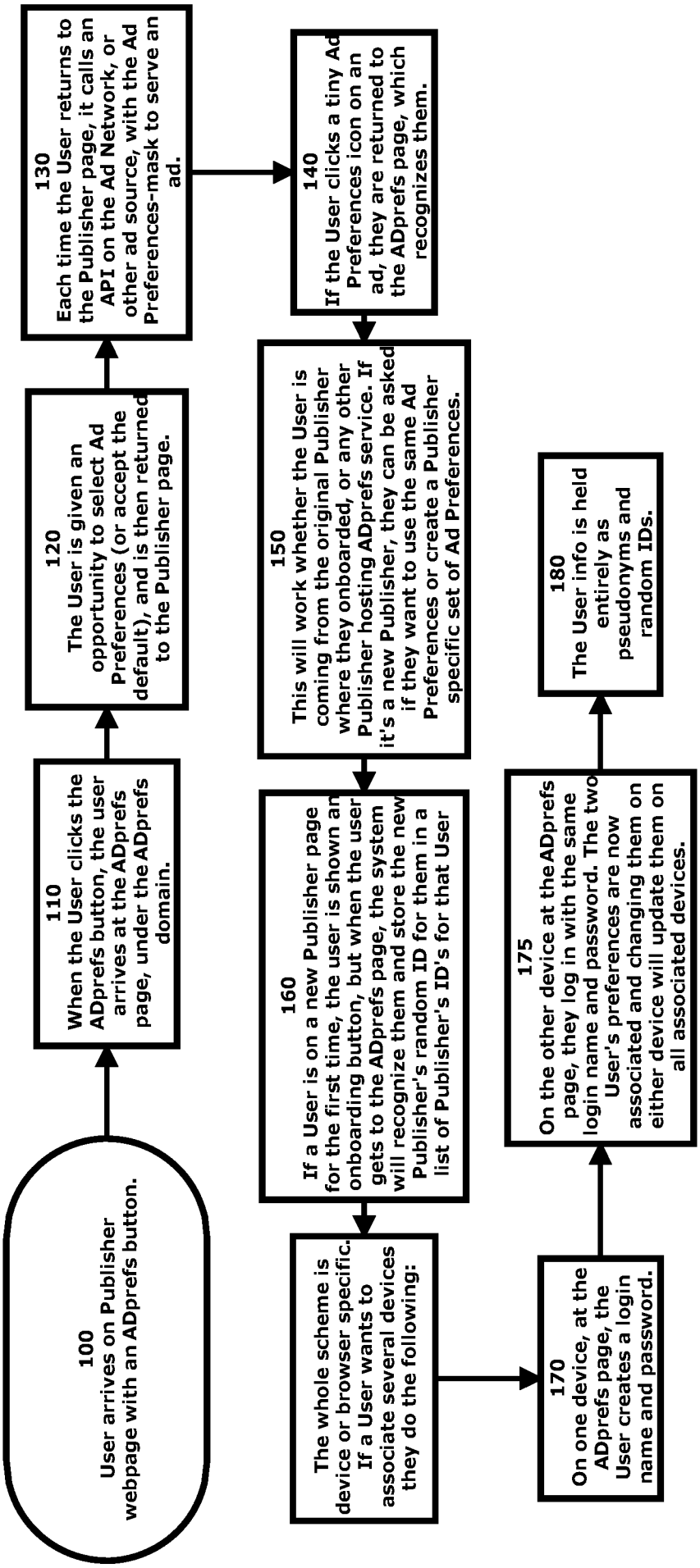
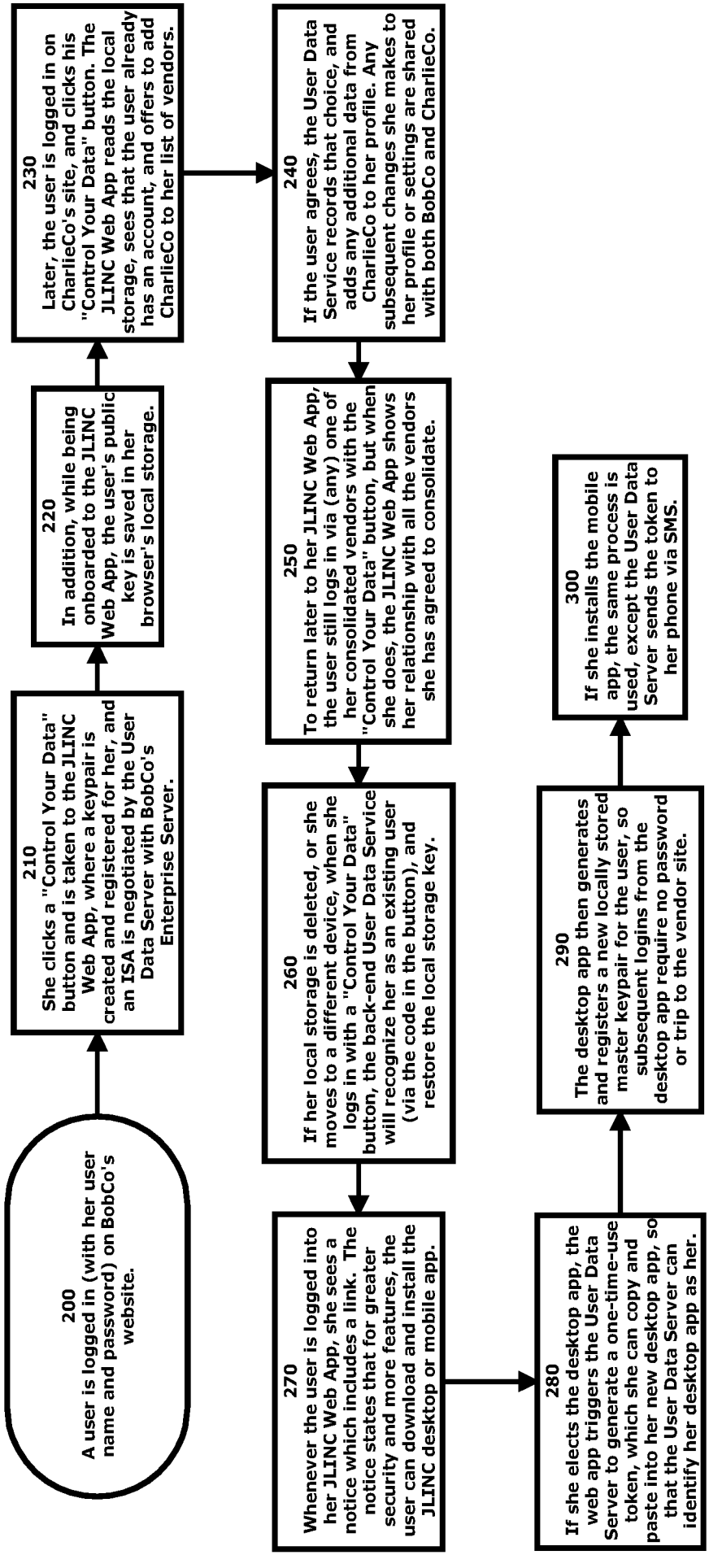

100
User arrives on Publisher webpage with an ADprefs button.
110
When the User clicks the ADprefs button, the user arrives at the ADprefs page, under the ADprefs domain.
120
The User is given an opportunity to select Ad Preferences (or accept the default), and is then returned to the Publisher page.
130
Each time the User returns to the Publisher page, it calls an API on the Ad Network, or other ad source, with the Ad Preferences-mask to serve an ad.
140
If the User clicks a tiny Ad Preferences icon on an ad, they are returned to the ADprefs page, which recognizes them.
150
This will work whether the User is coming from the original Publisher where they onboarded, or any other Publisher hosting ADprefs service. If it's a new Publisher, they can be asked if they want to use the same Ad Preferences or create a Publisher specific set of Ad Preferences.
160
If a User is on a new Publisher page for the first time, the user is shown an onboarding button, but when the user gets to the ADprefs page, the system will recognize them and store the new Publisher's random ID for them in a list of Publisher's ID's for that User
The whole scheme is device or browser specific. If a User wants to associate several devices they do the following:
170
On one device, at the ADprefs page, the User creates a login name and password.
175
On the other device at the ADprefs page, they log in with the same login name and password. The two User's preferences are now associated and changing them on either device will update them on all associated devices.
180
The User info is held entirely as pseudonyms and random IDs.

FIG. 4


200
A user is logged in (with her user name and password) on BobCo's website.
210
She clicks a "Control Your Data" button and is taken to the JLINC Web App, where a keypair is created and registered for her, and an ISA is negotiated by the User Data Server with BobCo's Enterprise Server.
220
In addition, while being onboarded to the JLINC Web App, the user's public key is saved in her browser's local storage.
230
Later, the user is logged in on CharlieCo's site, and clicks his "Control Your Data" button. The JLINC Web App reads the local storage, sees that the user already has an account, and offers to add CharlieCo to her list of vendors.
240
If the user agrees, the User Data Service records that choice, and adds any additional data from CharlieCo to her profile. Any subsequent changes she makes to her profile or settings are shared with both BobCo and CharlieCo.
250
To return later to her JLINC Web App, the user still logs in via (any) one of her consolidated vendors with the "Control Your Data" button, but when she does, the JLINC Web App shows her relationship with all the vendors she has agreed to consolidate.
260
If her local storage is deleted, or she moves to a different device, when she logs in with a "Control Your Data" button, the back-end User Data Service will recognize her as an existing user (via the code in the button), and restore the local storage key.
270
Whenever the user is logged into her JLINC Web App, she sees a notice which includes a link. The notice states that for greater security and more features, the user can download and install the JLINC desktop or mobile app.
280
If she elects the desktop app, the web app triggers the User Data Server to generate a one-time-use token, which she can copy and paste into her new desktop app, so that the User Data Server can identify her desktop app as her.
290
The desktop app then generates and registers a new locally stored master keypair for the user, so subsequent logins from the desktop app require no password or trip to the vendor site.
300
If she installs the mobile app, the same process is used, except the User Data Server sends the token to her phone via SMS.

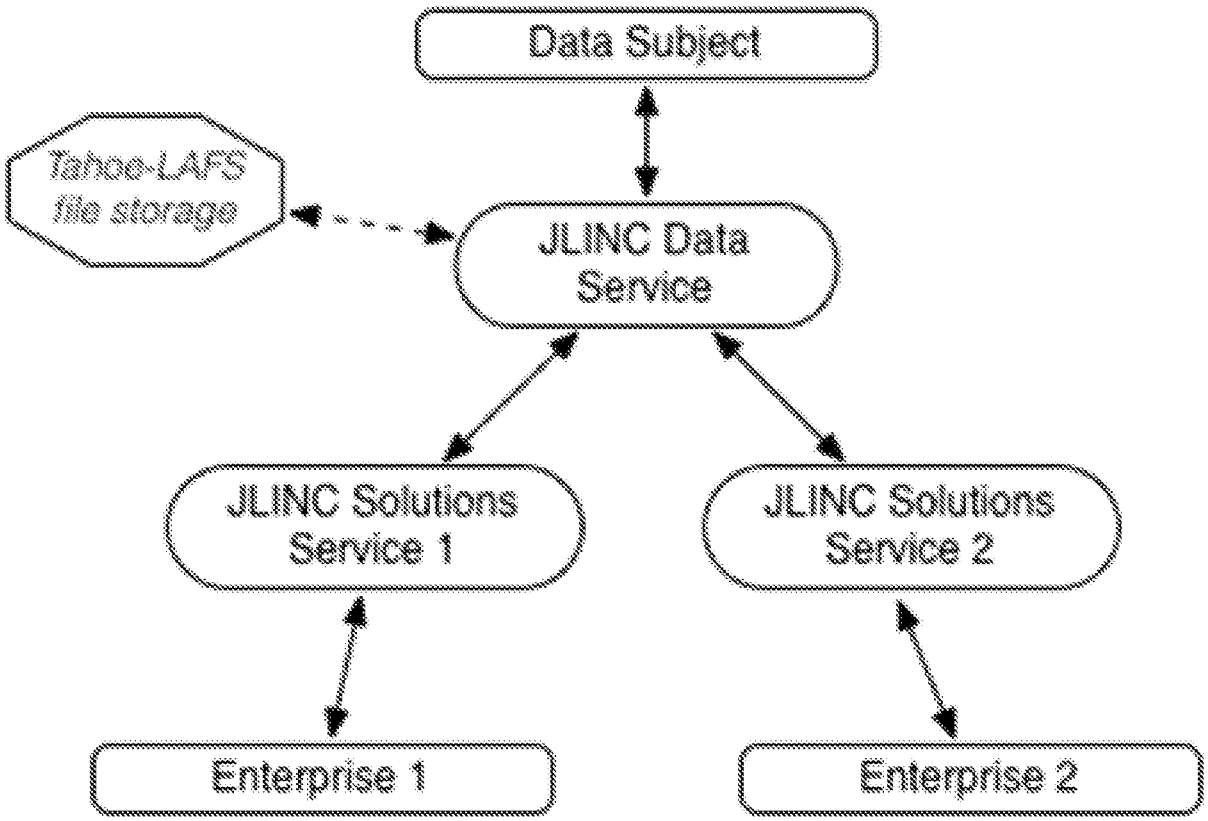

Data Subject
Tahoe-LAFS file storage
JLINC Data Service
JLINC Solutions Service 1
JLINC Solutions Service 2
Enterprise 1
Enterprise 2

FIG. 5