another person could have access to the user's account and, potentially, to the user's sensitive or confidential information or data. In addition, the more entities or individuals that a user shares their personal information with, the greater the risk of the user's information being stolen by a breach at one of the entities. Further, a user may only desire to share certain pieces of personal information with an entity or individual for limited purposes or limited in time.

[0005] Thus, it may be beneficial to provide exemplary systems and methods which allow users to control the use of user information to overcome at least some of the deficiencies described herein.

SUMMARY

[0006] Aspects of the disclosed technology include systems and methods for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device. Data access control may be provided in the context of personal user data, including handling requests to obtain access to personal user data via the interaction of a short-range transceiver, such as a contactless card, with a client device such that the personal user data is only provided to service providers who are authorized to review the data and disclosure of certain account identifier information, or account login information, need not be disclosed to service providers requesting access to personal user data.

[0006a] An aspect of the present disclosure provides a data access control system, comprising: a server comprising a processor and a memory, wherein the server is in data communication with a database and a client device, and wherein the server is configured to: receive, from the client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data, identify a user based on the user token, identify a service provider based on the service provider token, verify the service provider is authorized to receive access to the personal user data, retrieve the user key from the database,

generate the data access key based on the user key, and transmit the data access key to the client device.

[0006b] Another aspect of the present disclosure provides a method for controlling data access, comprising: receiving, from a first client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data stored on a contactless card associated with a user; identifying the user based on the user token; identifying a service provider based on the service provider token; verifying that the service provider is authorized to receive access to the personal user data stored on the contactless card; retrieving a user key associated with the user from a database; generating the data access key based on the user key; and transmitting the data access key to the first client device.

[0006c] Another aspect of the present disclosure provides a server, comprising: a processor; and a memory, wherein the server is in data communication with a database and a client device, and wherein the server is configured to: receive, from the client device, a user token, a service provider token, and a request for a data access key to decrypt encrypted personal user data, identify a user based on the user token, identify a service provider based on the service provider token, verify the service provider is authorized to receive access to the personal user data, retrieve the user key from the database, generate the data access key based on the user key, and transmit the data access key to the client device.

[0007] Embodiments of the present disclosure provide a data access control system, comprising: a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider; a server configured for data communication with a client device associated with the service provider; a contactless card associated with the user, the