[0004] Account access will often rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised, 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 creating and accessing a secure memory block in a client device via the interaction of a short-range transceiver, such as a contactless card, with a client device such that personal user data may be stored on a client device and remain protected from unauthorized access.

[0006a] According to an aspect, there is provided a method for controlling data access performed by a client application comprising instructions for execution on a client device, the client device having a secure memory block storing personal user data, the method comprising: receiving, from a contactless card, a user token; storing personal user data in the secure memory block; and encrypting the secure memory block using a data storage key.

[0006b] According to another aspect, there is provided a system for controlling data access, comprising a contactless card comprising a communications interface, a processor, and a memory, the memory storing a user token; and a client application comprising instructions

for execution on a client device, wherein the client application is configured to: receive, from the contactless card, the user token, transmit, to a server, the user token and a request for a data storage key, receive, from the server, the data storage key, create a secure memory block in a memory of the client device, store personal user data in the secure memory block, and encrypt the secure memory block using the data storage key.

[0006c] According to another aspect, there is provided a non-transitory machine-readable medium having stored thereon a client application comprising program code for execution on a client device, the client device having a secure memory block storing personal user data, the client application configured to, when executed, perform procedures comprising: receiving, from a contactless card, a user token; receiving, from a server, a data storage key; storing personal user data in the secure memory block; and encrypting the secure memory block using the data storage key.

[0007] Embodiments of the present disclosure provide a data access control system, comprising: a server configured for data communication with a client device associated with a user; a contactless card associated with the user, the contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token; a client application comprising instructions for execution on the client device, the client application configured to: in response a tap action between the contactless card and the client