

[00111] The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method for providing security services with respect to a remote cloud-based service, comprising in a security service provider module that is controlled by a first entity that is distinct from a second entity that controls the cloud-based service,

receiving a request from the cloud-based service to perform a security-related function including at least one of a storage or encryption operation, the request based on a policy that is specified by a user of the cloud-based service and that causes the cloud-based service to utilize the security service provider module to perform the security-related function; and

performing the security-related function on behalf of the cloud-based service.

2. The method of claim 1, wherein the request includes data to be stored by the security service provider module on behalf of the cloud-based service, and wherein performing the security-related function further comprises securely storing the data in the security service provider module.

3. The method of claim 2, further comprising causing the cloud-based service to delete the data, such that the data at rest is never stored by the cloud-based service.

4. The method of claim 1, wherein the request specifies data that is stored by the security service provider module on behalf of the cloud-based service, and wherein performing the security-related function further comprises:

retrieving the data; and

transmitting the retrieved data to the cloud-based service.

5. The method of claim 1, further comprising defining the policy, the policy controlling at least one of:

whether or not the cloud-based service should use the security service provider module to store data;

when the cloud-based service should provide data for storage by the security service provider module, based on state transitions and/or user activities occurring within the cloud-based service; and

removal of data resident on the cloud-based service based upon user activities, state transitions, and/or successful storage of the data by the security service provider module.

6. The method of claim 1, further comprising managing encryption keys that are operable to encrypt and decrypt data that is processed by the cloud-based service, such that the cloud-based service has no access to the encryption keys.

7. The method of claim 1, wherein the request includes data to be encrypted or decrypted by the security service provider module on behalf of the cloud-based service, and wherein performing the security-related function further comprises:

- encrypting or decrypting the data; and
- transmitting the encrypted or decrypted data to the cloud-based service.

8. The method of claim 1, wherein the request includes data to be decrypted by the security service provider module on behalf of the cloud-based service, and wherein performing the security-related function further comprises:

- decrypting the data; and
- transmitting the decrypted data to the user of the cloud-based service, such that the cloud-based service does not obtain access to the decrypted data at rest or in flight.

9. The method of claim 1, wherein the policy causes the cloud-based service provider to redirect to the security services provider module a user access to data stored by the cloud-based service, such that the user accesses the data from the services provider module in unencrypted form without the cloud-based service ever accessing the data in unencrypted form.

10. The method of claim 1, wherein the security services provider module performs encryption-related functions on encrypted data stored by the cloud-based service, and further comprising:

- receiving a request to restrict access by the cloud-based service to the encrypted data stored by the cloud-based service; and
- denying a subsequent request from the cloud-based service to decrypt the encrypted data, such that the data can no longer be accessed via the cloud-based service even though the cloud-based service still possesses one or more copies of the encrypted data.

11. The method of claim 1, wherein the cloud-based service is an electronic signature service.

12. The method of claim 11 wherein the request is a request to store an electronic signature document on behalf of the electronic signature service.

13. The method of claim 11, wherein the request is a request to encrypt or decrypt an electronic signature document on behalf of the electronic signature service.

14. A non-transitory computer-readable medium including instructions that, when executed by a computing system, provide security services with respect to a remote cloud-based service comprising in a security service provider module that is controlled by a first entity that is distinct from a second entity that controls the cloud-based service, the method comprising:

receiving a request initiated by the cloud-based service to perform a security-related function including at least one of a storage or encryption operation, the request based on a policy that is specified by a user of the cloud-based service and that causes the cloud-based service to utilize the security service provider module to perform the security-related function; and
performing the security-related function on behalf of the cloud-based service.

15. The computer-readable medium of claim 14, wherein the request is received from a device of a user of the cloud-based service, the request caused by a first redirection instruction transmitted from the cloud-based service to the device of the user, and wherein the method further comprises facilitating an upload of data to the cloud-based service, by:

receiving data from the device of the user;
encrypting the data according to the policy;
transmitting the encrypted data to the cloud service, thereby causing the cloud service to store the encrypted data; and
transmitting a second redirection instruction to the device of the user, the instruction causing the device to access the cloud-based-service to receive confirmation that the data was successfully uploaded to the cloud-based service.

16. The computer-readable medium of claim 15, wherein the method further comprises facilitating viewing of the uploaded data on the cloud-based service, by:

receiving a request from the device of the user, the request caused by a redirection instruction transmitted from the cloud-based service to the device of the user, the

redirection instruction including an identifier of the uploaded data and an associated key;

retrieving the uploaded data from the cloud-based service;

decrypting, based on the policy, the retrieved data; and

transmitting the decrypted data to the device of the user.

17. A computing system configured to provide security services with respect to a remote cloud-based service, the computing system controlled by an entity that does not control the remote cloud-based service, the computing system comprising:

a memory; and

a security services provider module that is stored on the memory and that is configured, when executed, to

define a policy specified by a user of the cloud-based service, the policy causing the cloud-based service to utilize the security service provider module to perform a security-related function;

receive a request initiated by the cloud-based service to perform the security-related function including at least one of a storage or encryption operation, the request based on the policy; and

perform the security-related function on behalf of the cloud-based service.

18. The computing system of claim 17, further comprising the cloud-based service, wherein the cloud-based service is configured to:

receive from the device of the user a request to upload data to the cloud-based service;

transmit a first redirection instruction to a device of the user, thereby causing the device of the user to transmit the request to the security services provider module;

wherein the security services provider module is further configured to:

receive the data from the device of the user;

encrypt the data according to the policy;

transmit the encrypted data to the cloud service, thereby causing the cloud service to store the encrypted data; and

transmit a second redirection instruction to the device of the user, the instruction causing the device to access the cloud-based-service to receive confirmation that the data was successfully uploaded to the cloud-based service.

19. The computing system of claim 18, wherein the cloud-based service is further configured to:

receive from the device of the user a request to access the uploaded data;
in response to the request, transmit a redirection instruction to the device of the user, thereby causing the device of the user to transmit a request to access the uploaded data to the security services provider module, the redirection instruction including an identifier of the uploaded data and an associated key;

wherein the security services provider module is further configured to:

receive from the device of the user the request to access the uploaded data, the request including the identifier of the uploaded data and associated key;
retrieve the uploaded data from the cloud-based service;
decrypt, based on the policy, the retrieved data; and
transmit the decrypted data to the device of the user, without passing through the cloud-based service.

20. The computing system of claim 18, wherein the cloud-based service never accesses the uploaded data in unencrypted form.

21. The computing system of claim 18, wherein the request to upload data is an HTTP request, and wherein the first and second redirection instructions are HTTP redirect instructions.

22. The computing system of claim 17, further comprising a policy that specifies that a document stored by the cloud-based service is to be made opaque to the cloud-based service upon occurrence of a specified document state, and wherein the security services provider module is further configured to:

monitor state changes to the document by consulting the policy to determine whether the specified document state has occurred;
before occurrence of the specified document state, decrypt the document on behalf of the cloud-based service; and
after occurrence of the specified document state, refuse to decrypt the document on behalf of the cloud-based service, thereby rendering the document opaque to the cloud-based service.

23. The computing system of claim 17, wherein the cloud-based service is an electronic signature service, and wherein the security services provider module is configured to:

process a request to store an electronic signature document on behalf of the electronic signature service; and

process a request to encrypt or decrypt an electronic signature document on behalf of the electronic signature service.

24. The computing system of claim 23, wherein the security services provider module is operated by a customer of the electronic signature service, such that the security-related functions are performed under control of the customer and not the electronic signature service.

25. The computing system of claim 17, wherein the policy comprises a save policy vector that specifies a data type, a data state or operation, and a data escrow location, wherein the data escrow location selects between storage at the cloud-based service and storage by the security service provider.

26. The computing system of claim 17, wherein the cloud-based service is a digital transaction service.

CLAIMS

1. A system for protecting stored data accessed by a cloud-based service platform, the system comprising:

- a network connection;
- a working memory device;
- a persistent data storage medium;

one or more processors coupled to the working memory device, the network connection and the persistent data storage medium, the persistent data storage medium containing instructions that, when executed on the system, cause the system to perform operations including:

- receiving, over the network connection, a document as part of a service request from a first user of the cloud-based service platform;

- maintaining the document within the working memory device, without writing the document to the persistent data storage medium;

- transmitting, over the network connection, the document to a security service provider for persistent storage;

- deleting the document from the working memory device in response to receiving a confirmation of receipt of the document from the security service provider;

- determining, after deleting the document, that a pending action associated with performance of the service request requires access to the document;

- receiving in response to a request, over the network connection using the one or more processors, the document from the security service provider;

- in response to receiving the document, maintaining the document within the working memory device, without writing the document to the persistent data storage medium;

- performing, using the one or more processors, one or more actions involving the document in satisfaction of at least part of the service request, the one ore more actions including the pending action; and

- upon completion of the one or more actions involving the document, deleting the document from the working memory device.

2. The system of claim 1, wherein the determining that the pending action requires access to the document includes receiving a signature completion request from a second user.
3. The system of claim 2, wherein the performing the one or more actions includes presenting at least a representation of the document to the second user for signature.
4. The system of claim 3, wherein the performing the one or more actions includes receiving signature data from the second user representative of the second user applying a digital or electronic signature to the document.
5. The system of claim 4, wherein the persistent storage medium further comprises instructions that cause the system to perform the operation of storing the signature data in association with the document and the service request prior to deleting the document from the working memory.
6. The system of claim 1, wherein the performing the one or more actions includes collecting and maintaining metadata confirming the one or more actions associated with the document and the service request.
7. The system of claim 1, wherein the deleting the document from working memory device occurs in response to the following conditions:
 - no actions associated with the service request requiring access to the document are pending processing on the cloud-based service platform; and
 - receipt of a confirmation from the security service provider of receipt and storage of a current copy of the document.
8. The system of claim 1, wherein the receiving the document as part of a service request includes:
 - accessing a policy associated with the first user;

evaluating the service request and the document against the policy; and
determining whether to persistently store the document with the security service provider based on results of evaluating the service request and document.

9. The system of claim 8, wherein evaluating the service request and the document against the policy includes evaluating a status associated with the document against the policy.

10. A method for protecting stored data accessed by a cloud-based service platform, the method comprising:

on a computing system within the cloud-based document management service platform performing operations including:

receiving, over a network connection using one or more processors, a document as part of a service request from a first user of the cloud-based service platform;

transmitting, over the network connection using the one or more processors, the document to a security service provider for persistent storage;

deleting the document from the cloud-based service platform in response to receiving a confirmation of receipt of the document from the security service provider;

determining, after deleting the document, that a pending action associated with performance of the service request requires access to the document;

receiving in response to a request, over the network connection using the one or more processors, the document from the security service provider;

performing, using the one or more processors, one or more actions involving the document in satisfaction of at least part of the service request, the one or more actions including the pending action; and

upon completion of the one or more actions involving the document, deleting the document from the cloud-based service platform for at least a second time.

11. The method of claim 10, wherein the determining that the pending action requires access to the document includes receiving a signature completion request from a second user.

12. The method of claim 11, wherein the performing the one or more actions includes presenting at least a representation of the document to the second user for signature.

13. The method of claim 12, wherein the performing the one or more actions includes receiving signature data from the second user representative of the second user applying a digital or electronic signature to the document.

14. The method of claim 13, further comprising storing the signature data in association with the document and the service request prior to deleting the document from the cloud-based service platform.

15. The method of claim 10, wherein the performing the one or more actions includes collecting and maintaining metadata confirming the one or more actions associated with the document and the service request.

16. The method of claim 10, wherein the deleting the document from the cloud-based service platform occurs in response to the following conditions:

no actions associated with the service request requiring access to the document are pending processing on the cloud-based service platform; and

receipt of a confirmation from the security service provider of receipt and storage of a current copy of the document.

17. The method of claim 10, wherein the receiving the document as part of a service request includes:

accessing a policy associated with the first user;

evaluating the service request and the document against the policy; and

determining whether to persistently store the document with the security service provider based on results of evaluating the service request and document.

18. The method of claim 17, wherein evaluating the service request and the document against the policy includes evaluating a status associated with the document against the policy.

19. A non-transitory computer-readable storage medium containing instructions that, when executed on a computer system within a cloud-based service platform, cause the computer system to perform operations including:

- receiving, over a network connection, a document as part of a service request from a first user of the cloud-based service platform;

- maintaining the document within a working memory portion of the computer system, without writing the document to a persistent data storage within the cloud-based service platform;

- transmitting, over the network connection, the document to a security service provider for persistent storage;

- deleting the document from the working memory portion in response to receiving a confirmation of receipt of the document from the security service provider;

- determining, after deleting the document, that a pending action associated with performance of the service request requires access to the document;

- receiving in response to a request, over the network connection using the one or more processors, the document from the security service provider;

- in response to receiving the document, maintaining the document within the working memory portion, without writing the document to the persistent data storage;

- performing, using the one or more processors, one or more actions involving the document in satisfaction of at least part of the service request, the one or more actions including the pending action; and

- upon completion of the one or more actions involving the document, deleting the document from the working memory portion.

20. The non-transitory computer-readable storage medium of claim 19, wherein the determining that the pending action requires access to the document includes receiving a signature completion request from a second user; and

wherein the performing the one or more actions includes presenting at least a representation of the document to the second user for signature.

21. The non-transitory computer-readable storage medium of claim 19, wherein performing the one or more actions includes collecting and maintaining metadata confirming the one or more actions associated with the document and the service request.

22. The non-transitory computer-readable storage medium of claim 19, wherein the deleting the document from working memory device occurs in response to the following conditions:

no actions associated with the service request requiring access to the document are pending processing on the cloud-based service platform; and

receipt of a confirmation from the security service provider of receipt and storage of a current copy of the document.