[0004] Still more problems arise. Even if an individual or enterprise organization implements true best practices (such as cold storage data access and management), encryption and/or decryption information still needs to regularly change and multiple backup copies must be kept. Indeed, in an enterprise environment, multiple copies are required in several secure locations, with single use addresses/keys/passwords and proper management of current version control in each location after encryption/re-encryption. Challenges also exist with the enforcement of data security policies governing retrieval and use of private keys/passwords, making sure that no single person (not even the CEO) may individually retrieve sensitive data.

SUMMARY

[0004a] According to a first aspect of the present invention, there is provided a method executed by a device that encrypts an electronic data, the method comprising: receiving, by the device, passwords associated with users, each password of the passwords associated with a corresponding user of the users; receiving, by the device, a first selection representing a minimum number of the multiple passwords; receiving, by the device, a second selection of the electronic data to encrypt; generating, by the device, an encryption vault key using only the passwords as inputs to a key derivation function; generating, by the device, an encrypted version of the electronic data represented by the second key selection by encrypting the electronic data using the encryption vault key generated using only the passwords; generating, by the device, vault key secret shares by inputting the encryption vault key, the passwords, and the minimum number to a secret sharing algorithm; receiving, by the device, a request to change at least one of the passwords; in response to the receiving of the request to change the at least one of the passwords, receiving, by the device, the minimum number of the vault key secret shares; creating, by the device, a recreated version of the encryption vault key using the minimum number of the vault key secret shares; receiving, by the device, new passwords associated with new users; and generating, by the device, new vault key secret shares of the recreated version of the encryption vault key by inputting the recreated version of the encryption vault key, the new passwords, and the minimum number to the secret sharing algorithm; wherein the at least one of the passwords is changed without decrypting the encrypted version of the electronic data.

[0004b] According to a second aspect of the present invention, there is provided a system encrypting an electronic data, comprising: a hardware processor; and a memory device storing instructions that when executed by the hardware processor perform operations, the operations comprising: receiving a first selection via a graphical user interface of a number of authorized individuals required for an encryption of the electronic data; receiving passwords entered by the authorized individuals via the graphical user interface, each password of the passwords entered by a corresponding individual of the authorized individuals; receiving a second selection via the graphical user interface representing a minimum number of the passwords that are required for a decryption operation; generating a cryptographic vault key by inputting only the passwords and the minimum number of the passwords as inputs to a key derivation function; generating an encrypted version of the electronic data by encrypting the electronic data using the cryptographic vault key an encryption parameter to an encryption algorithm; generating vault key secret shares by inputting the cryptographic vault key, the passwords, and the minimum number to a secret sharing algorithm; receiving a change request via the graphical user interface to change at least one password of the passwords entered by the corresponding individual; in response to the receiving of the change request, receiving the minimum number of the vault key secret shares; creating a recreated version of the cryptographic vault key using the minimum number of the vault key secret shares; receiving new passwords associated with new authorized individuals; and generating new secret shares of the recreated version of the cryptographic vault key by inputting the recreated version of the cryptographic vault key, the new passwords, and the minimum number to the secret sharing algorithm; wherein the at least one password is changed without decrypting the encrypted version of the electronic data.

[0004c] According to a third aspect of the present invention, there is provided a memory device storing instructions that, when executed by a hardware processor, facilitate performance of operations that encrypt an electronic data, the operations comprising: receiving a request via a graphical user interface to execute an encryption operation; prompting via the graphical user interface to input a number *N* of authorized individuals that are required for an encryption operation; in response to the prompting to input the number of the authorized individuals, receiving a first selection via the graphical user interface representing the number *N* of the authorized individuals required for the encryption operation; prompting via the graphical user interface to

input multiple identity credentials; in response to the prompting to input the multiple identity credentials, receiving passwords and biometric inputs, each password of the passwords and each biometric input of the biometric inputs entered by a corresponding individual of the authorized individuals; prompting via the graphical user interface to input a minimum number; in response to the prompting to input the minimum number, receiving a second selection via the graphical user interface representing the minimum number; deriving a cryptographic key using only the passwords, the biometric inputs and the minimum number as inputs to a key derivation function; generating an encrypted version of the electronic data by encrypting the electronic data using the cryptographic key; generating key secret shares by inputting the cryptographic key, the passwords and the minimum number to a secret sharing algorithm; receiving a request via the graphical user interface to change at least one of the passwords; receiving new passwords associated with new authorized individuals; receiving the minimum number of the key secret shares; creating a recreated version of the cryptographic key using the minimum number of the key secret shares; and generating new secret shares of the recreated version of the cryptographic key by inputting the recreated version of the cryptographic key, the new passwords, and the minimum number to the secret sharing algorithm; wherein the passwords are changed without decrypting the encrypted version of the electronic data.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0005] The features, aspects, and advantages of the exemplary embodiments are understood when the following Detailed Description is read with reference to the accompanying drawings, wherein:

FIGs. 1-13 are simplified illustrations of a multi-user credential mechanism for protecting an electronic data, according to exemplary embodiments;

FIGs. 14-15 are more detailed illustration of an operating environment, according to exemplary embodiments;

FIGs. 16-22 are screenshots illustrating an encryption operation, according to exemplary embodiments;

FIGs. 23-25 are screenshots illustrating a creation of a vault key, according to exemplary embodiments;

FIGs. 31-34 are screenshots illustrating a decryption operation, according to exemplary embodiments;

FIG. 35 is a flowchart illustrating a method or algorithm for encryption of the electronic data, according to exemplary embodiments;

FIG. 36 is a flowchart illustrating a method or algorithm for decryption of encrypted data, according to exemplary embodiments;

FIG. 37 illustrates biometric encryption, according to exemplary embodiments;

FIGs. 38-43 are additional screenshots illustrating menu configurations, according to exemplary embodiments; and

CLAIMS

1. A method executed by a ~~computer~~ device that encrypts an electronic data, the method comprising:

receiving, by ~~a computer~~the device, ~~capacitive inputs representing multiple~~ passwords associated with ~~multiple~~ users, each password of the ~~multiple~~ passwords associated with a corresponding user of the ~~multiple~~ users;

receiving, by the device, a first selection representing a minimum number of the multiple passwords;

receiving, by the ~~computer~~device, a ~~capacitive~~ second selection ~~representing~~ of the electronic data to encrypt;

generating, by the ~~computer~~device, an encryption vault key using only the ~~capacitive inputs representing the multiple~~ passwords as inputs to a key derivation function; ~~and~~

generating, by the ~~computer~~device, an encrypted version of the electronic data represented by the second key selection by encrypting the electronic data using the encryption vault key ~~as an encryption parameter to an encryption algorithm~~generated using only the passwords;

generating, by the device, vault key secret shares by inputting the encryption vault key, the passwords, and the minimum number to a secret sharing algorithm;

receiving, by the device, a request to change at least one of the passwords;

in response to the receiving of the request to change the at least one of the passwords, receiving, by the device, the minimum number of the vault key secret shares;

creating, by the device, a recreated version of the encryption vault key using the minimum number of the vault key secret shares;

receiving, by the device, new passwords associated with new users; and

generating, by the device, new vault key secret shares of the recreated version of the encryption vault key by inputting the recreated version of the encryption vault key, the new passwords, and the minimum number to the secret sharing algorithm;

wherein the at least one of the passwords is changed without decrypting the encrypted version of the electronic data.

2. The method of claim 1, further comprising ~~storing the vault key~~receiving inputs representing the passwords associated with the users.

3. The method of claim 1, further comprising prompting to enter ~~for~~ the ~~multiple~~ passwords ~~entered by the multiple users~~.

~~4. The method of claim 1, further comprising providing only the vault key and a minimum number of the multiple passwords as inputs to a secret sharing algorithm.~~

~~5~~4. The method of claim 1, further comprising receiving an output selection to output a physical version of the encryption vault key.

~~6~~5. The method of claim 1, further comprising receiving an output selection to output a physical version of the encrypted version of the electronic data.

~~7~~6. The method of claim 1, further comprising ~~avoiding a cache miss by caching the vault key to a processor cache memory~~storing the encryption vault key.

~~8~~7. A system ~~that encrypts~~encrypting an electronic data, comprising:

a hardware processor; and

a memory device storing instructions that when executed by the hardware processor perform operations, the operations comprising:

receiving a first selection via a graphical user interface of a number of authorized individuals required for an encryption of ~~an~~ the electronic data;

receiving ~~multiple~~ passwords entered by the authorized individuals via the graphical user interface, each password of the ~~multiple~~ passwords entered by a corresponding individual of the ~~number of the~~ authorized individuals ~~required for the encryption of the electronic data~~;

receiving a second selection via the graphical user interface representing a minimum number of the ~~multiple~~ passwords that are required for a decryption operation;

generating a cryptographic vault key by inputting only the ~~multiple~~ passwords and the minimum number of the passwords as inputs ~~entered by the authorized individuals~~ to a key derivation function;

generating an encrypted version of the electronic data by encrypting the electronic data using ~~only~~ the cryptographic vault key ~~as~~ an encryption parameter to an encryption algorithm; ~~and~~

generating vault key secret shares by inputting the cryptographic vault key, the passwords, and the minimum number to a secret sharing algorithm;

receiving a change request via the graphical user interface to change at least one password of the passwords entered by the corresponding individual;

in response to the receiving of the change request, receiving the minimum number of the vault key secret shares;

creating a recreated version of the cryptographic vault key using the minimum number of the vault key secret shares;

receiving new passwords associated with new authorized individuals; and

generating new secret shares of the recreated version of the cryptographic vault key by inputting the recreated version of the cryptographic vault key, the new passwords, and the minimum number to the secret sharing algorithm;

wherein the at least one password is changed without decrypting the encrypted version of the electronic data~~secret sharing the cryptographic vault key by inputting only the cryptographic vault key and the minimum number of the multiple passwords to a secret sharing algorithm~~.

~~9~~8. The system of claim ~~8~~7, wherein the operations further comprise receiving inputs representing the ~~multiple~~ passwords ~~entered by the multiple users~~.

~~10~~9. The system of claim ~~8~~7, wherein the operations further comprise prompting for the ~~multiple~~ passwords ~~entered by the multiple users~~.

~~11. The system of claim 8, wherein the operations further comprise changing any password of the multiple passwords without executing the decryption operation that decrypts the encrypted version of the electronic data.~~

~~12~~10. The system of claim ~~8~~7, wherein the operations further comprise receiving an output selection to output a physical version of the cryptographic vault key~~changing the cryptographic vault key without decrypting the encrypted version of the electronic data~~.

~~13~~11. The system of claim ~~8~~7, wherein the operations further comprise receiving an output selection to output a physical version of the encrypted version of the electronic data.

~~14~~12. The system of claim ~~8~~7, wherein the operations further comprise storing the cryptographic vault key.

~~15~~13. The system of claim ~~8~~7, wherein the operations further comprise storing, by the system, the encrypted version of the electronic data.

~~16~~14. A memory device storing instructions that, when executed by a hardware processor, facilitate performance of operations that encrypt an electronic data, the operations comprising:

receiving a request via a graphical user interface to execute an encryption operation;

prompting via the graphical user interface to input a number *N* of authorized individuals that are required for an encryption ~~of an electronic data~~operation;

in response to the prompting to input the number ~~N~~ of the authorized individuals, receiving a first selection via the graphical user interface representing the number *N* of the authorized individuals required for the encryption ~~of the electronic data~~operation;

prompting via the graphical user interface to input multiple identity credentials;

in response to the prompting to input the multiple identity credentials, receiving ~~multiple~~ passwords and ~~multiple~~ biometric inputs, each password of the ~~multiple~~ passwords and each biometric input of the ~~multiple~~ biometric inputs entered by a

corresponding individual of the authorized individuals ~~required for the encryption of the electronic data~~;

prompting via the graphical user interface to input a minimum number ~~of the multiple identity credentials that are required for a decryption operation~~;

in response to the prompting to input the minimum number, receiving a second selection via the graphical user interface representing the minimum number ~~of the multiple identity credentials that are required for the decryption operation~~;

deriving ~~an encryption vault~~a cryptographic key using only the ~~multiple~~ passwords, ~~and~~ the ~~multiple~~ biometric inputs and the minimum number as inputs to a key derivation function;

generating an encrypted version of the electronic data by encrypting the electronic data using the ~~encryption vault~~cryptographic key ~~as an encryption parameter to a n encryption algorithm~~; ~~and~~

generating key secret shares ~~of the encryption vault key~~ by inputting ~~only~~ the ~~encryption vault~~cryptographic key, the passwords and the minimum number ~~of the multiple identity credentials that are required for the decryption operation~~ to a secret sharing algorithm;

receiving a request via the graphical user interface to change at least one of the passwords;

receiving new passwords associated with new authorized individuals;

receiving the minimum number of the key secret shares;

creating a recreated version of the cryptographic key using the minimum number of the key secret shares; and

generating new secret shares of the recreated version of the cryptographic key by inputting the recreated version of the cryptographic key, the new passwords, and the minimum number to the secret sharing algorithm;

wherein the passwords are changed without decrypting the encrypted version of the electronic data.

~~17. The memory device of claim 16, wherein the operations further comprise distributing the secret shares of the encryption vault key.~~

~~18. The memory device of claim 16, wherein the operations further comprise sending the secret shares of the encryption vault key to Internet protocol addresses associated with the number *N* of the authorized individuals.~~

~~19. The memory device of claim 16, wherein the operations further comprise generating a decryption key based on the secret shares of the encryption vault key.~~