Claims

1. A method for storing a first data object, comprising:

decomposing, by applying a decomposition function, the first data object into a first fragment associated with a first original record locator and a second fragment associated with a second original record locator;

obfuscating the first original record locator to generate a first obfuscated record locator and the second original record locator to generate a second obfuscated record locator;

encrypting the first fragment using a first encryption key and the second fragment using a second encryption key; and

storing, to at least a first of a plurality of storage locations, the first encrypted fragment with the corresponding first obfuscated record locator and the second encrypted fragment with the second obfuscated record locator, and

selecting the decomposition function based at least in part on one or more variable storage parameters.

2. The method of claim 1, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

3. The method of claim 1, further comprising varying the one or more variable storage parameters in response to detecting a trigger.

4. The method of claim 3, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

5. The method of claim 1, further comprising determining the first encryption key based at least in part on the first original record locator and the second encryption key based at least in part on the second original record locator.

6. The method of claim 5, wherein the first encryption key and the second encryption key are further determined based at least in part on one or more variable storage parameters.

7. The method of claim 6, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

8. The method of claim 6, further comprising varying the one or more variable storage parameters in response to detecting a trigger.

9. The method of claim 8, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

10. The method of claim 1, further comprising obfuscating each of the first fragment and the second fragment prior to encrypting the first fragment and the second fragment.

11. The method of claim 1, wherein the first fragment and the second encryption key are encrypted using the first encryption key, the second fragment and a third encryption key are encrypted using the second encryption key, and the third encryption key is used to encrypt a third fragment of the first data object.

12. The method of claim 1, wherein obfuscating each of the first original record locator and the second original record locator comprises:

altering each of the first original record locator and the second original record locator; and

applying an obfuscation function to each of the first original record locator and the second original record locator.

13. The method of claim 12, wherein each of the first original record locator and the second original record locator are obfuscated based at least in part on one or more variable storage parameters.

14. The method of claim 13, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

15. The method of claim 13, further comprising varying the one or more variable storage parameters in response to detecting a trigger.

16. The method of claim 15, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

17. The method of claim 1, further comprising identifying at least the first of the plurality of storage locations to store the first encrypted fragment with the corresponding first obfuscated record locator and the second encrypted fragment with the second obfuscated record locator based at least in part on one or more variable storage parameters.

18. The method of claim 17, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

19. The method of claim 17, further comprising varying the one or more variable storage parameters in response to detecting a trigger.

20. The method of claim 1, further comprising generating a data map that includes one or more of an index of a sequence of the first fragment and the second fragment of the first

data object, the first encryption key and the second encryption key, the first obfuscated record locator and the second obfuscated record locator, and at least the first of the plurality of storage locations.

21. The method of claim 20, further comprising encrypting the data map and storing the encrypted data map.

22. The method of claim 20, further comprising varying a content of the data map based at least in part on one or variable storage parameters.

23. The method of claim 22, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

24. A system for storing a first data object, comprising:

a plurality of storage locations;

a secure platform comprising one or more processors coupled to memory configured to:

decompose the first data object into a first fragment associated with a first original record locator and a second fragment associated with a second original record locator;

obfuscate the first original record locator to generate a first obfuscated record locator and the second original record locator to generate a second obfuscated record locator;

encrypt the first fragment using a first encryption key and the second fragment using a second encryption key; and

store, to at least a first of the plurality of storage locations, the first encrypted fragment with the corresponding first obfuscated record locator and the second encrypted fragment with the second obfuscated record locator,

wherein to decompose the first data object, the one or more processors are configured to apply a decomposition function, and

wherein the one or more processors are further configured to select the decomposition function based at least in part on one or more variable storage parameters.

25. The system of claim 24, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

26. The system of claim 24, wherein the one or more processors are further configured to vary the one or more variable storage parameters in response to detecting a trigger.

27. The system of claim 26, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

28. The system of claim 24, wherein the one or more processors are further configured to determine the first encryption key based at least in part on the first original record locator and the second encryption key based at least in part on the second original record locator.

29. The system of claim 28, wherein the one or more processors are configured to determine the first encryption key and the second encryption key further based at least in part on one or more variable storage parameters.

30. The system of claim 29, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

31. The system of claim 29, wherein the one or more processors are further configured to vary the one or more variable storage parameters in response to detecting a trigger.

32. The system of claim 31, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

33. The system of claim 24, wherein the one or more processors are further configured to obfuscate each of the first fragment and the second fragment prior to encrypting the first fragment and the second fragment.

34. The system of claim 24, wherein the first fragment and the second encryption key are encrypted using the first encryption key, the second fragment and a third encryption key are encrypted using the second encryption key, and the third encryption key is used to encrypt a third fragment of the first data object.

35. The system of claim 24, wherein to obfuscate each of the first original record locator and the second original record locator, the one or more processors are configured to:

alter each of the first original record locator and the second original record locator; and

apply an obfuscation function to each of the first original record locator and the second original record locator.

36. The system of claim 35, wherein the one or more processors are further configured to obfuscate each of the first original record locator and the second original record locator based at least in part on one or more variable storage parameters.

37. The system of claim 36, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

38. The system of claim 36, wherein the one or more processors are further configured to vary the one or more variable storage parameters in response to detecting a trigger.

39. The system of claim 38, wherein the trigger comprises a security breach with respect to one or more of the first data object, a second data object, the first of the plurality of storage locations, and a second of the plurality of storage locations.

40. The system of claim 24, wherein the one or more processors are further configured to identify at least the first of the plurality of storage locations to store the first encrypted fragment with the corresponding first obfuscated record locator and the second encrypted fragment with the second obfuscated record locator based at least in part on one or more variable storage parameters.

41. The system of claim 40, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.

42. The system of claim 40, wherein the one or more processors are further configured to vary the one or more variable storage parameters in response to detecting a trigger.

43. The system of claim 24, wherein the one or more processors are further configured to generate a data map that includes one or more of an index of a sequence of the first fragment and the second fragment of the first data object, the first encryption key and the second encryption key, the first obfuscated record locator and the second obfuscated record locator, and at least the first of the plurality of storage locations.

44. The system of claim 43, wherein the one or more processors are further configured to encrypt the data map and store the encrypted data map.

45. The system of claim 43, wherein the one or more processors are further configured to vary a content of the data map based at least in part on one or variable storage parameters.

46. The system of claim 45, wherein the one or more variable storage parameters include at least one of a username, a user passphrase, a current security model, a type of the first data object, a size of the first data object, one or more security requirements, and one or more performance requirements.