

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2021-114100

(P2021-114100A)

(43) 公開日 令和3年8月5日(2021.8.5)

|                                |               |             |
|--------------------------------|---------------|-------------|
| (51) Int.Cl.                   | F 1           | テーマコード (参考) |
| <b>G 0 6 F 21/62 (2013.01)</b> | G 0 6 F 21/62 |             |
| <b>G 0 6 F 21/60 (2013.01)</b> | G 0 6 F 21/60 | 3 2 O       |
| <b>G 0 6 F 21/33 (2013.01)</b> | G 0 6 F 21/60 | 3 4 O       |
|                                | G 0 6 F 21/33 |             |

審査請求 未請求 請求項の数 7 O L (全 8 頁)

|           |                          |          |                         |
|-----------|--------------------------|----------|-------------------------|
| (21) 出願番号 | 特願2020-6224 (P2020-6224) | (71) 出願人 | 000208891               |
| (22) 出願日  | 令和2年1月17日 (2020.1.17)    |          | K D D I 株式会社            |
|           |                          |          | 東京都新宿区西新宿二丁目 3 番 2 号    |
|           |                          | (74) 代理人 | 100106002               |
|           |                          |          | 弁理士 正林 真之               |
|           |                          | (74) 代理人 | 100120891               |
|           |                          |          | 弁理士 林 一好                |
|           |                          | (72) 発明者 | 清本 晋作                   |
|           |                          |          | 埼玉県ふじみ野市大原二丁目 1 番 1 5 号 |
|           |                          |          | 株式会社 K D D I 総合研究所内     |
|           |                          | (72) 発明者 | 仲野 有登                   |
|           |                          |          | 埼玉県ふじみ野市大原二丁目 1 番 1 5 号 |
|           |                          |          | 株式会社 K D D I 総合研究所内     |

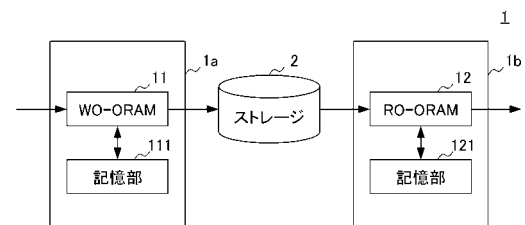
(54) 【発明の名称】 ファイル管理システム、ファイル管理方法及びファイル管理プログラム

## (57) 【要約】

【課題】 ユーザ毎に、所定のストレージへのデータの書き込み又は読み込みのみを許可できるセキュアなファイル管理システム、ファイル管理方法及びファイル管理プログラムを提供すること。

【解決手段】 ファイル管理システム 1 は、暗号化されたストレージ 2 に対するアクセスパターンを保護し、ストレージ 2 への書き込みのみが可能な WO-ORAM (11) と、ストレージ 2 に対するアクセスパターンを保護し、ストレージ 2 からの読み込みのみが可能な RO-ORAM (12) と、を備え、WO-ORAM (11) は、ストレージ 2 への書き込みを許可するユーザを登録し、当該ユーザの認証を行い、RO-ORAM (12) は、ストレージ 2 からの読み込みを許可するユーザを登録し、当該ユーザの認証を行う。

【選択図】 図 1



**【特許請求の範囲】****【請求項 1】**

暗号化されたストレージに対するアクセスパターンを保護し、当該ストレージへの書き込みのみが可能な書き込み制御部と、

前記ストレージに対するアクセスパターンを保護し、当該ストレージからの読み込みのみが可能な読み込み制御部と、を備え、

前記書き込み制御部は、前記ストレージへの書き込みを許可するユーザを登録し、当該ユーザの認証を行い、

前記読み込み制御部は、前記ストレージからの読み込みを許可するユーザを登録し、当該ユーザの認証を行うファイル管理システム。

10

**【請求項 2】**

前記書き込み制御部は、前記ストレージの中で、データが格納されていない空の領域を特定し、当該空の領域に書き込みを行う請求項 1 に記載のファイル管理システム。

**【請求項 3】**

前記書き込み制御部は、ユーザ毎の書き込み可能回数を制限する請求項 1 又は請求項 2 に記載のファイル管理システム。

**【請求項 4】**

前記読み込み制御部は、ファイルのインデックスとして前記書き込み制御部により付与された日時情報に基づいて、読み込みの対象ファイルを特定する請求項 1 から請求項 3 のいずれかに記載のファイル管理システム。

20

**【請求項 5】**

前記書き込み制御部及び前記読み込み制御部は、登録するユーザ毎に公開鍵証明書及び秘密鍵を発行し、前記公開鍵証明書、及び前記秘密鍵による署名により当該ユーザの認証を行う請求項 1 から請求項 4 のいずれかに記載のファイル管理システム。

**【請求項 6】**

書き込み制御部が暗号化されたストレージに対するアクセスパターンを保護し、当該ストレージへの書き込みのみを行う書き込み制御ステップと、

読み込み制御部が前記ストレージに対するアクセスパターンを保護し、当該ストレージからの読み込みのみを行う読み込み制御ステップと、を含み、

前記書き込み制御ステップにおいて、前記書き込み制御部は、予め前記ストレージへの書き込みを許可されたユーザの認証を行い、

30

前記読み込み制御部ステップにおいて、前記読み込み制御部は、予め前記ストレージからの読み込みを許可されたユーザの認証を行うファイル管理方法。

**【請求項 7】**

請求項 1 から請求項 5 のいずれかに記載のファイル管理システムとしてコンピュータを機能させるためのファイル管理プログラム。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、データアクセスパターンを保護するセキュアなファイル管理システム、ファイル管理方法及びファイル管理プログラムに関する。

40

**【背景技術】****【0002】**

従来、メモリに対するアクセスパターンが解析されることにより、様々な情報が漏洩し得ることが示されており、プログラム保護の観点からアクセスパターンを保護することが望まれている。

アクセスパターンを保護するための手法としては、ORAM (O b l i v i o u s R A M) が知られている (例えば、非特許文献 1 参照)。また、ORAM において読み込みのみを許可し、書き込みを禁止するといった制御を実装した方式も提案されている (例えば、非特許文献 2 参照)。

50

【先行技術文献】

【非特許文献】

【0003】

【非特許文献1】Kai-Min Chung and Rafael Pass: A Simple ORAM, IACR Cryptology ePrint Archive, 2013/243 (2013).

【非特許文献2】Shruti Tople, Yaoqi Jia and Prateek Saxena: PRO-ORAM: Constant Latency Read-Only Oblivious RAM, Cryptology ePrint Archive, 2018/220 (2018).

10

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、従来のORAMによるアクセス制御では、全てのユーザが読み込みのみしかできない等、ファイルの格納及び利用の用途によって不都合が生じていた。

【0005】

本発明は、ユーザ毎に、所定のストレージへのデータの書き込み又は読み込みのみを許可できるセキュアなファイル管理システム、ファイル管理方法及びファイル管理プログラムを提供することを目的とする。

【課題を解決するための手段】

20

【0006】

本発明に係るファイル管理システムは、暗号化されたストレージに対するアクセスパターンを保護し、当該ストレージへの書き込みのみが可能な書き込み制御部と、前記ストレージに対するアクセスパターンを保護し、当該ストレージからの読み込みのみが可能な読み込み制御部と、を備え、前記書き込み制御部は、前記ストレージへの書き込みを許可するユーザを登録し、当該ユーザの認証を行い、前記読み込み制御部は、前記ストレージからの読み込みを許可するユーザを登録し、当該ユーザの認証を行う。

【0007】

前記書き込み制御部は、前記ストレージの中で、データが格納されていない空の領域を特定し、当該空の領域に書き込みを行ってもよい。

30

【0008】

前記書き込み制御部は、ユーザ毎の書き込み可能回数を制限してもよい。

【0009】

前記読み込み制御部は、ファイルのインデックスとして前記書き込み制御部により付与された日時情報に基づいて、読み込みの対象ファイルを特定してもよい。

【0010】

前記書き込み制御部及び前記読み込み制御部は、登録するユーザ毎に公開鍵証明書及び秘密鍵を発行し、前記公開鍵証明書、及び前記秘密鍵による署名により当該ユーザの認証を行ってもよい。

【0011】

40

本発明に係るファイル管理方法は、書き込み制御部が暗号化されたストレージに対するアクセスパターンを保護し、当該ストレージへの書き込みのみを行う書き込み制御ステップと、読み込み制御部が前記ストレージに対するアクセスパターンを保護し、当該ストレージからの読み込みのみを行う読み込み制御ステップと、を含み、前記書き込み制御ステップにおいて、前記書き込み制御部は、予め前記ストレージへの書き込みを許可されたユーザの認証を行い、前記読み込み制御部ステップにおいて、前記読み込み制御部は、予め前記ストレージからの読み込みを許可されたユーザの認証を行う。

【0012】

本発明に係るファイル管理プログラムは、前記ファイル管理システムとしてコンピュータを機能させるためのものである。

50

## 【発明の効果】

## 【0013】

本発明によれば、ユーザ毎に、所定のストレージへのデータの書き込み又は読み込みのみを許可できるセキュアなファイルシステムを構成できる。

## 【図面の簡単な説明】

## 【0014】

【図1】実施形態におけるファイル管理システムの機能構成を示す図である。

【図2】実施形態におけるユーザ認証及びストレージへのアクセスの手順を示すシーケンス図である。

## 【発明を実施するための形態】

10

## 【0015】

以下、本発明の実施形態の一例について説明する。

図1は、本実施形態におけるファイル管理システム1の機能構成を示す図である。

## 【0016】

本実施形態のファイル管理システム1は、クラウドサーバ等、外部のサーバに構成されたストレージ2に対して、データの書き込み及び読み込みを行う。企業のゲートウェイ等、信頼できるネットワークのエンドポイントに制御装置又は制御装置群(1a、1b、…)が設けられて構成される。

## 【0017】

ファイル管理システム1には、メモリ上のデータへのアクセスパターンを秘匿可能な、ORAMと呼ばれる制御部が複数実装される。これらの制御部は、書き込み制御部としてのWO-ORAM(11)と、読み込み制御部としてのRO-ORAM(12)とに分類される。

20

WO-ORAM(11)は、データの書き込みのみが可能に、RO-ORAM(12)は、データの読み込みのみが可能に構成される。

## 【0018】

WO-ORAM(11)及びRO-ORAM(12)の方式は限定されないが、一例として、square root solutionによる動作を示す。

## 【0019】

square root solutionでは、元のn個のデータに対して、shelterと呼ばれるルートn個のデータを保管できる領域と、さらに、ルートn個のダミーブロックとが追加される。その後、n+ルートn個のデータに対して、ORAMのプログラムのみが知る規則 $\pi$ に応じて並び替えが行われる。これにより、アドレスiのデータは、アドレス $\pi(i)$ に保管されることになる。

30

## 【0020】

ORAMがアドレスiに保管されているデータに対してアクセスを行う場合、まず、shelter内の全データに対してアクセスを行い、該当のデータが含まれているかどうかを判定する。

該当のデータが含まれていない場合、ORAMは、 $\pi(i)$ に対してアクセスを行い、データをshelterにコピーする。一方、該当のデータが含まれている場合には、ORAMは、 $\pi(d+t)$ にアクセスを行い、 $(d+t)$ に保管されるデータをshelterにコピーする。

40

ここで、dはダミーのアドレス、tは何回目のアクセスかを表すカウンタである。また、ORAMは、一定期間毎にshuffleと呼ばれる処理を実施し、データの攪拌と再構成とを行う。

## 【0021】

WO-ORAM(11)及びRO-ORAM(12)は、ユーザ認証のためのユーザ情報を、記憶部111及び121にそれぞれ格納し、ユーザからの書き込み要求又は読み込み要求に対してユーザ認証を行う。すなわち、記憶部111に登録されたユーザのみがWO-ORAM(11)を介して、ストレージ2にデータを書き込み、記憶部121に登録

50

されたユーザのみが R O - O R A M ( 1 2 ) を介して、ストレージ 2 からデータを読み込む。

【 0 0 2 2 】

なお、ストレージ 2 のデータは、所定の方式により暗号化されており、s h e l t e r にデータが展開された際に復号されるものとする。すなわち、W O - O R A M ( 1 1 ) は、ユーザデータを暗号化してストレージ 2 に書き込み、R O - O R A M ( 1 2 ) は、読み込んだデータを復号してユーザに提供する。暗号方式には、例えば共通鍵暗号が用いられ、W O - O R A M ( 1 1 ) 及び R O - O R A M ( 1 2 ) に同じ鍵が埋め込まれる。

【 0 0 2 3 】

W O - O R A M ( 1 1 ) 及び R O - O R A M ( 1 2 ) によるユーザ認証の手順は限定されないが、一例として、公開鍵を用いた認証手順を示す。 10

図 2 は、本実施形態におけるユーザ認証及びストレージ 2 へのアクセスの手順を示すシーケンス図である。

なお、図中の O R A M は、W O - O R A M ( 1 1 ) 又は R O - O R A M ( 1 2 ) のいずれかを指す。

【 0 0 2 4 】

ステップ S 1 において、O R A M は、登録したユーザ毎に、公開鍵証明書及び秘密鍵を発行する。これらは、所定の方式により該当のユーザに安全に提供される。

【 0 0 2 5 】

ステップ S 2 において、O R A M は、ユーザの端末から、ストレージ 2 に対する読み込み又は書き込みを行うためのアクセス要求を受け付ける。 20

【 0 0 2 6 】

ステップ S 3 において、O R A M は、乱数を生成してユーザの端末に送信する。

ステップ S 4 において、ユーザの端末は、受信した乱数に対して秘密鍵で署名を行い、この署名と共に、公開鍵証明書を O R A M へ送信する。

【 0 0 2 7 】

ステップ S 5 において、O R A M は、公開鍵証明書の正当性を確認し、さらに、署名の検証を行う。

【 0 0 2 8 】

ステップ S 6 において、O R A M は、ユーザの代理として、ストレージ 2 にアクセスし、データの書き込み又は読み込みを行う。 30

O R A M は、データを読み込んだ場合、ステップ S 7 において、このデータをユーザの端末に返送する。

【 0 0 2 9 】

なお、O R A M とユーザの端末との間の認証のプロトコルは、例えば T L S ( T r a n s p o r t L a y e r S e c u r i t y ) のクライアント認証等、既存の方式が用いられてもよい。

【 0 0 3 0 】

次に、W O - O R A M ( 1 1 ) 及び R O - O R A M ( 1 2 ) における、データアクセスに関する拡張機能について説明する。 40

【 0 0 3 1 】

W O - O R A M ( 1 1 ) は、データの上書きを避けるための W r i t e ワンスの機能を実現する手法として、ストレージ 2 の中で、データが格納されていない空の領域を特定し、この空の領域に書き込みを行う。

例えば、W O - O R A M ( 1 1 ) は、まず適当なダミーアクセスを含めてストレージ 2 上の複数のブロックにアクセスし、s h e l t e r にデータを展開する。続いて、W O - O R A M ( 1 1 ) は、展開されたデータを確認し、データが格納されていないブロックを特定し、特定した空のブロックに書き込みたいデータを埋め込む。

【 0 0 3 2 】

このとき、ブロックのヘッダ部分に乱数が付与され、また、W O - O R A M ( 1 1 ) は 50

、展開した他のブロックについても、ヘッダ部分の乱数を別の乱数に置き換えて更新する。その後、shelter上のデータは、全てシャッフルされて、ストレージ2に戻される。戻される際には、暗号化されるが、ヘッダ部分の乱数が更新されるため、全て別の暗号文となって書き込まれる。

#### 【0033】

また、WO-ORAM(11)は、ユーザ認証の際に、記憶部111に格納されているユーザ情報に含まれるユーザ毎の書き込み可能回数を確認し、上限に達していない場合にのみストレージ2への書き込みを許可すると共に、書き込み回数を更新する。これにより、WO-ORAM(11)は、ユーザ毎の書き込み可能回数を制限する。

#### 【0034】

RO-ORAM(12)は、ストレージ2に格納されるファイルのインデックスとしてWO-ORAM(11)により付与された日時情報に基づいて、読み込みの対象ファイルを特定する。このように、ORAM間で統一されたインデックスを共有することにより、最新の正しいファイルが読み込まれ、ユーザに提供される。

#### 【0035】

本実施形態によれば、ファイル管理システム1は、暗号化されたストレージに対するアクセスパターンを秘匿するための、書き込み専用のWO-ORAM(11)と、読み込み専用のRO-ORAM(12)とを備え、各ORAMがユーザ認証により利用ユーザを限定する。

したがって、従来は、いずれのユーザも書き込みと読み込みとが可能となっていたところ、ファイル管理システム1は、ユーザ毎に、ストレージ2へのデータの書き込み又は読み込みのみを許可できる。

#### 【0036】

また、ストレージ2に格納されるデータは、暗号化されると共に、攪拌されるため、正規のORAMを経由しなければ正しく書き込み及び読み込みができない。さらに、アクセスパターンが秘匿されることにより、ファイル管理システム1は、ユーザ毎に読み書きの可否を制御可能なセキュアなシステムを構成できる。

この結果、例えば、あるシステムのログデータをセキュアに保管し、必要に応じて管理者のみが検証できる仕組みが構築できる。この場合、システムはログデータの書き込みのみを行い、管理者は読み込みだけが許可されてログデータの書き換えができない。

#### 【0037】

ファイル管理システム1は、ストレージ2の中で、データが格納されていない空の領域を特定し、この空の領域に書き込みを行う。

したがって、ファイル管理システム1は、格納済みのデータを上書きすることがなく、Writeワンスの仕組みを実現できる。

#### 【0038】

ファイル管理システム1は、ユーザ毎の書き込み可能回数を制限することにより、ユーザのアクセス権限を詳細に制御できる。

#### 【0039】

ファイル管理システム1は、書き込みの日時情報をインデックスとして読み込みの対象ファイルを特定するので、複数のORAMの間でインデックスが共有され、読み書きの整合性が確保される。

#### 【0040】

ファイル管理システム1は、登録するユーザ毎に公開鍵証明書及び秘密鍵を発行し、公開鍵証明書、及び秘密鍵による署名によりユーザの認証を行う。

したがって、ファイル管理システム1は、正規のユーザを適切に認証し、書き込み又は読み込みの可否を正しく制御できる。

#### 【0041】

以上、本発明の実施形態について説明したが、本発明は前述した実施形態に限るものではない。また、前述した実施形態に記載された効果は、本発明から生じる最も好適な効果

10

20

30

40

50

を列挙したに過ぎず、本発明による効果は、実施形態に記載されたものに限定されるものではない。

【0042】

前述の実施形態では、ファイル管理システム1は、複数のORAMがゲートウェイに配置される構成としたが、各部の配置はこれには限られない。また、一部の構成が分散配置されてもよく、例えば、square root solutionにおけるshelterがユーザの端末に設けられてもよい。

【0043】

また、ファイル管理システム1は、書き込み専用のWO-ORAM(11)、及び読み込み専用のRO-ORAM(12)がそれぞれ1つずつ設けられた構成としたが、これには限られず、それぞれが複数設けられてもよい。さらに、読み書き両方が可能なORAMが追加されてもよい。

10

【0044】

ファイル管理システム1によるファイル管理方法は、ソフトウェアにより実現される。ソフトウェアによって実現される場合には、このソフトウェアを構成するプログラムが、情報処理装置(コンピュータ)にインストールされる。また、これらのプログラムは、CD-ROMのようなリムーバブルメディアに記録されてユーザに配布されてもよいし、ネットワークを介してユーザのコンピュータにダウンロードされることにより配布されてもよい。さらに、これらのプログラムは、ダウンロードされることなくネットワークを介したWebサービスとしてユーザのコンピュータに提供されてもよい。

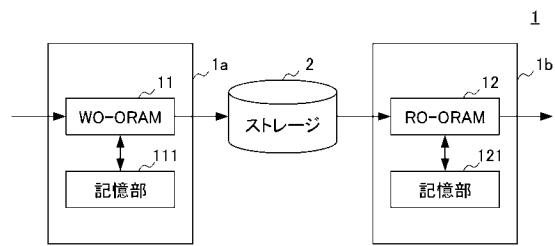
20

【符号の説明】

【0045】

- 1 ファイル管理システム
- 2 ストレージ
- 11 WO-ORAM
- 12 RO-ORAM
- 111 記憶部
- 121 記憶部

【図 1】



【図 2】

