科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２２　日現在

機関番号：　１１３０１
研究種目：　若手研究(B)
研究期間：　2012～2013
課題番号：　２４７０００５８

研究課題名（和文）オフライン行動履歴を事後検証可能かつ安全にクラウド上に記録し活用する技術の開発

研究課題名（英文）Development of a method for secure recording off-line activities on cloud strage with ex-post verifiable format and utilizing it

研究代表者
酒井　正夫（SAKAI, MASAO）

東北大学・教育情報基盤センター・准教授

研究者番号：３０３４４７４０

交付決定額（研究期間全体）：（直接経費）　　1,000,000円、（間接経費）　　300,000円

研究成果の概要（和文）：本研究では，モバイル端末ユーザのオフライン行動履歴のクラウド上での記録と活用に資するために，複数の個人向けクラウドストレージと秘密分散共有法を利用してクラウドストレージに強固に安全にデータを記録する技術を開発した。
また，今回の開発技術を実装したWindowsアプリを作成し，一般的なユーザの利用を想定した際の安全性評価と，転送速度などの定量的性能評価を行った。

研究成果の概要（英文）：In this study, we have developed a method for secure recording off-line activities of smartphone users on cloud storage with ex-post verifiable format and utilizing it. In addition, we have also developed application softwares based on the developed method and evaluated the performance of it. Under the circumstances, data stored in the cloud storage have risks such as steal and falsification of it, because users need to delegate their data authority to the service provider of the cloud storage. In order to avoid the risks, the developed method divides encrypted data to multiple shares by using Secret-Sharing (SS) and upload them to different multiple cloud storages.

研究分野：　総合領域

科研費の分科・細目：　情報学・計算機システム・ネットワーク

キーワード：　クラウド　秘密分散共有法　オフライン行動履歴　ソフトウェア

１．研究開始当初の背景

近年，スマートフォンの高性能化とクラウド型ウェブサービスの普及により，屋外でも日常的にインターネットを利用するユーザが増大している．そのようなモバイルユーザを対象として適切な行動ターゲティング広告を表示するためには，ユーザのオフライン（実社会）での行動を収集し分析することが重要になる．実際，世界最大のオンライン広告会社である Google 社は，2006 年に「ユーザのデータを（オンラインに限定せず）100%集めることが目標」と公言しており，2008 年からはそれに資するスマートフォン用 OS『Android』を開発している．また,『iPhone』を開発する Apple 社は，2010 年よりモバイル端末ユーザを対象とした広告表示サービス『iAd』を開始しており，さらに，iPhone がユーザの位置情報を無断で収集して暗号化せずに保存していることが判明している．このように，主要なインターネット関連企業は，既にユーザのオフライン行動履歴の収集に取り組み始めている．

しかし，ユーザの行動履歴は，本来，保護されるべきプライバシ情報であり，企業が安易に取り扱って良いものではない．例えば，2011 年 9 月，女性が男性パートナーの行動（位置，通話記録，電池残量など）を秘密裏に監視できる Android アプリ『カレログ』（http://karelog.jp/）に対する批判がインターネット上で高まり，開発会社がウェブサイト上で謝罪して一部の機能を停止する事態が起こっている．このように，ユーザの行動履歴を本人以外が無断で収集・使用するようなサービスは，セキュリティとプライバシに関して重大な問題を有している．

一方で，これまでにない画期的で優れたサービスを創造する可能性も秘めている．したがって，本人から許諾を得て収集したオフライン行動履歴を，セキュリティとプライバシに十分配慮して，本人自身が閲覧・使用する用途においては，その有効な活用策を積極的に検討すべきである．例えば，スマートフォンなどのモバイル端末がユーザの 24 時間 365 日のオフライン行動履歴（位置，動作，周囲の状況など）を自動収集し，本人が日時や項目別に整理して閲覧できるようになるだけでも，備忘録や日記として便利に利用可能である．また，行動履歴を，第三者が事後にその正確性を検証可能なデータとして記録できるならば，ユーザは自己の過去の行動を第三者に証明する手段を獲得することになる．このことは，冤罪容疑などでのアリバイの証明や，ネット掲示板や SNS などでの自己の発信情報の正しさを証明する手段として役立つと期待できる．さらに，本人のみがその正確性を容易に検証できるという行動履歴の特性から，そのデータはチャレンジ&レスポンス型ユーザ認証用のチャレンジ問題の作成に活用できる可能性がある．

申請者は，「事後にその正確性を検証可能な行動履歴」のことを，「『そのユーザ本人の記録であること』,『その時刻に記録されたこと』,『唯一であること（矛盾するデータが同時に存在しないこと）』の三つを第三者が事後に納得できる行動履歴」と定義している．行動履歴をそのようなデータとして記録する関連技術として，これまでに申請者と研究協力者らは，複数のモジュール同士が連携して，相互に動作を監視し合うことでモジュール動作の正常/異常を判別し，危殆化しているモジュールを安全に修復する技術を開発している．

本研究では，この関連技術を援用することで，複数のユーザが連携して，行動履歴の正確性の検証とそのデータに対するディジタル署名を相互に行う技術の開発を試みる．連携するユーザ数が十分大きい場合には，P2P 型サービスと同様に専用サーバを必要とせず，事後にその正確性を検証可能な行動履歴の記録が可能になると期待できる．

また，申請者は，行動履歴データからチャレンジ&レスポンス型ユーザ認証用のチャレンジ用問題を安全に自動作成するために検索可能暗号の技術を援用することを検討している．検索可能暗号とは，復号を経ずにキーワード検索が可能な暗号化を実現する技術である．チャレンジ問題は行動履歴データの内容をもとに作成されるため，通常は，その問題作成プログラムに行動履歴の暗号データを復号する権限と機能を付与する必要がある．そのため，問題作成プログラムやそれが動作するクラウドサーバがハッキングされた場合に，ユーザの行動履歴の内容が第三者に漏洩するリスクが生じる．しかし，行動履歴データの暗号化と問題作成の処理に検索可能暗号の技術を導入することで，このリスクを大幅に低減できる可能性がある．

２．研究の目的

本研究では，スマートフォンなどのモバイル端末で自動収集されるユーザのオフライン行動履歴を，事後にその正確性を検証可能なデータとしてクラウド上のオンラインストレージに安全に記録する技術を開発する．さらに，その行動履歴のデータを活用して，そのデータに含まれるユーザ本人しか知りえない情報をもとに，チャレンジ&レスポンス型ユーザ認証用のチャレンジ問題を安全に自動作成する技術も開発する．また，スマートフォンなどのモバイル端末と各種クラウド型サービスの利用を前提に，開発した技術の安全性と有効性を，計算機シミュレーションなども利用して検証・評価する．

具体的な目標を箇条書きすると以下のようになる．

- 収集・記録・使用に適したオフライン行動履歴のデータ構造と操作プロトコルを決定する．
- 事後の検証とキーワード検索が可能な暗号データとして行動履歴を記録する

技術を開発する．

- 行動履歴の暗号データから，安全に，チャレンジ問題を自動作成する技術を開発する．
- 開発した技術の安全性を理論的に検証し，有効性を計算機シミュレーションにより評価する．

３．研究の方法

オフライン行動履歴を安全かつ効率的にクラウドストレージ上に収集・記録する際に，ユーザ自身が行うセキュリティ対策としては，保存データを暗号化することが一般的である．しかし，警察レベルの強力な権限と調査力を持つ攻撃者に狙われた場合，複数のサービスでパスワードを使いまわす大多数の一般ユーザの安全性は容易に破綻する．また，データの消失に暗号化は無力である．

そこで，より高レベルな対策として，図１のように，保存データを秘密分散法により分割する方法が考えられる．秘密分散法によりデータを複数の異なるクラウドストレージ上に分散して保存すれば，一部のクラウドストレージが敵に奪われた場合にも，元データを守ることができる．

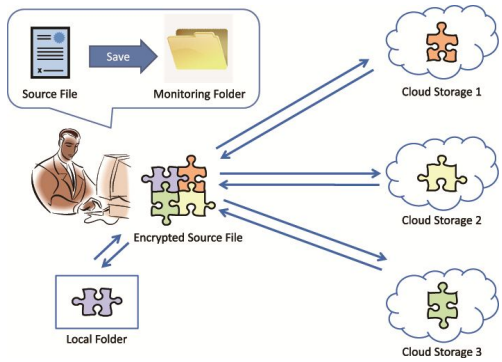

図１：秘密分散法による処理イメージ

既に，この方法を用いた法人ユーザ向けの有償サービス（NRI セキュアテクノロシーズ社「SecureCube/SecretShare」など）が存在する．しかし，それらはデータの分散/復号処理に専用サーバを必要とし，使用できるクラウドストレージが限定されるなど，高性能かつ高コストなサービスがほとんどであり，個人ユーザの使用には適さない．また，それらが使用するアプリケーション（以後，アプリ）のソースコードは通常非公開なため，その安全性を客観的に検証することが不可能である．個人ユーザ向けには，ユーザの端末上で動作するアプリにより同様の機能の実現を目指す「MyCloud プロジェクト（http://sourceforge.jp/projects/mycloud/)」が存在する．しかし，2013 年 12 月 16 日現在，そのようなアプリの一般公開には至っていない．

そこで，研究代表者らは，秘密分散法によりクラウドストレージを安全に活用する技術の実用化研究の一環として，ユーザの端末と複数の汎用クラウドストレージのみで動作する個人向け Windows アプリを作成した．そして，その作成アプリを一般ユーザが利用する場合に起こりえる危険な状況を想定した安全性検証を行い，その結果判明した潜在リスクの対処方法を検討した．さらに，dropbox，Google ドライブ，OneDrive などの主要のクラウドストレージサービスと連携した場合の実際の転送速度などの定量的性能評価も行った。

４．研究成果

複数の個人向けクラウドストレージと秘密分散共有法を利用してクラウドストレージに強固に安全にデータを記録する 3SoC (Secret Sharing Scheme on Cloud)技術を開発し，また，その動作検証用に，ローカルストレージのデータを秘密分散法により複数のクラウドストレージに自動バックアップする基本アプリ（図２）と，その基本アプリを発展させたメモ帳のアプリ（図３）を作成した．

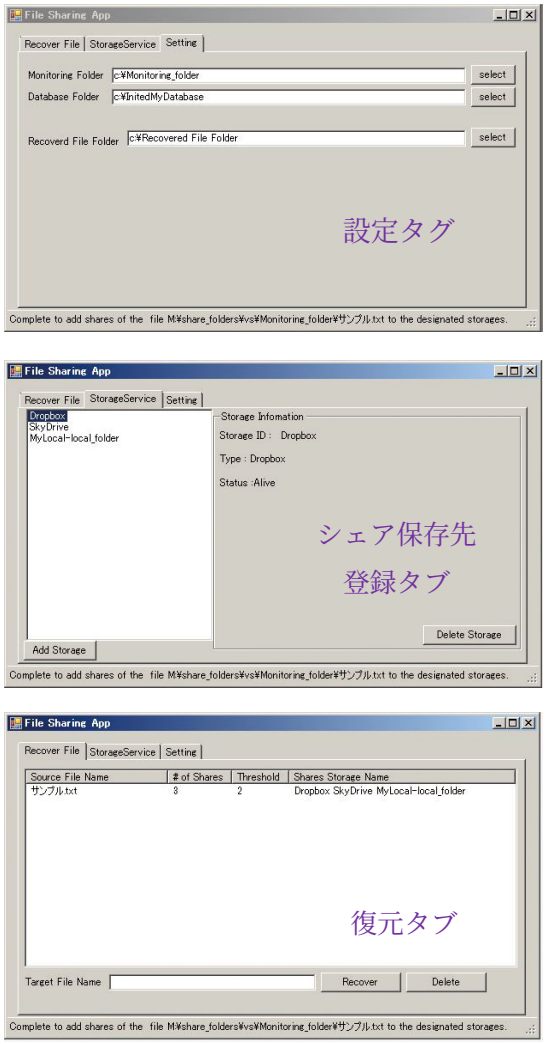

図２：基本アプリの画面構成

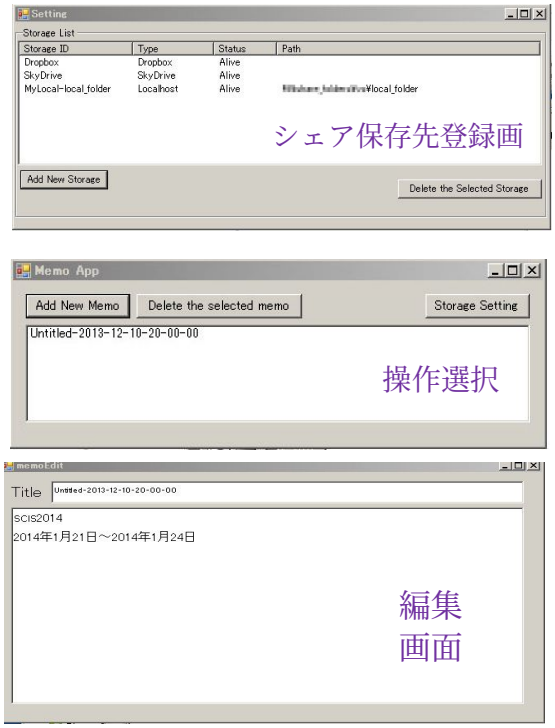

図３：発展アプリ（メモ帳）の画面構成

さらに，この Windows アプリの一般的な利用形態における仮想的な安全性検証を行い，その優れた有用性と将来性を示した。この成果は，2014 年 1 月開催の「2014 年 暗号と情報セキュリティシンポジウム(SCIS 2014)」にて発表を行った。

また，この汎用クラウドストレージサービス（Dropbox，OneDrive，Google Drive）を利用した場合の、Windows アプリの性能評価も行った.その結果、この Windows アプリが、現状で十分な実用性を有することを示し、さらに、汎用クラウドストレージサービスの特性を考慮することで更なる性能向上が期待できることも示した。この成果の詳細は，2014 年 10 月開催の国際会議「the International Symposium on Information Theory and Its Applications (ISITA2014)」に発表予定である。

本研究で開発した 3SoC 技術は，クラウドストレージに保存するデータに、情報理論的安全性を実現するものである。現在のところ，このような製品・サービスは法人向けに限定されており，一般ユーザ向けには実用的かつオープンな製品がまだ存在しない。したがって，本研究で作成した Windows アプリを一般に公開することには、大きな意義があると言える。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0 件）
〔学会発表〕（計　2 件）

1．　福光正幸、長谷川真吾、岩崎淳也、酒井正夫,高橋大樹、秘密分散法によりクラウドストレージを安全に活用する技術の実用化研究、SCIS2014 暗号と情報セキュリティシンポジウム、2014 年 1 月 23 日、鹿児島市
2．　Masayuki Fukumitsu, Shingo Hasegawa, Junya Iwazaki, Masao Sakai, and Daiki Takahashi, Development of a Method using Encryption and Secret Sharing for Making Cloud Storage Secure and its Application, the International Symposium on Information Theory and Its Applications (ISITA2014), 2014 年 10 月 29 日,オーストラリア・メルボルン (under review)

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　０件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www.isl.is.tohoku.ac.jp/sss/

６．研究組織
(1)研究代表者
酒井 正夫（MASAO SAKAI）
東北大学・教育情報基盤センター・准教授
研究者番号：30344740

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：