科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１４　日現在

機関番号：　１２１０１
研究種目：　基盤研究(C)
研究期間：　2010～2013
課題番号：　２２５０００８０

研究課題名（和文）Ｐ２Ｐを利用したロバストなログストレージに関する研究

研究課題名（英文）A Study on a Robust Log Storage based on P2P network

研究代表者
大瀧　保広（Ohtaki, Yasuhiro）

茨城大学・IT基盤センター・准教授

研究者番号：３０２６１７３８

交付決定額（研究期間全体）：（直接経費）　　1,900,000円、（間接経費）　　570,000円

研究成果の概要（和文）：P2Pに基づくログストレージは、分散ファイルシステム上に対改ざん性を持つログストレージを構成することで実現される。ログメッセージは暗号化されて分散保管され、ログの閲覧は検索可能暗号化による。P2Pではノードがプロトコルを遵守しない恐れがあるため、ログストレージとして機能するためには、ノードが不正な処理を行った場合、それを検出できる機構が必要である。ノードが不正を行った場合に検出できる方式を提案したが、非常に計算コストが高いものとなった。実用にはまだ改善の余地がある。

研究成果の概要（英文）：Robust Log storage based on P2P network can be constructed by building tamper resistant log storage system on a P2P distributed file system. Each log message are first converted into several shares by secret sharing scheme. Then each share are encrypted with symmetric searchable encryption (SSE) scheme and then stored on some P2P nodes. Since P2P nodes could not assumed to be honest, we need a scheme which can verify that each node followed the scheme correctly. We proposed a verifiable SSE scheme and a verifiable dynamic SSE scheme. We've implemented prototype system. We found that the dynamic scheme require very high computation cost on each peer, and thus it is not yet feasible for practical use.

研究分野：　総合領域

科研費の分科・細目：　情報学・情報学基礎

キーワード：　検索可能暗号　監査ログ　Dynamic SSE

１．研究開始当初の背景

デジタルな電磁記録は、書き換えた時に「書き換えた痕跡」が残らないため、改ざんされたのか、もともとそのようなデータなのかの判別ができない。デジタル情報に「証拠能力」を持たせるためには、改ざんの痕跡が残る仕組みを人為的に作り込んで置く必要がある。デジタル情報に人為的に証拠能力を持たせる研究分野は「Digital Evidence」と呼ばれる。Digital Evidence の一分野として改ざんを防止するシステムログの研究分野があり「Secure Audit Log」などと呼ばれる。

一方で、P2P ネットワーク上に分散配置された情報は、消去が困難であるという性質がある。この性質は、アーカイブやログ記録を目的とするストレージとしては望ましい。

暗号化された形で記録された情報の中から、欲しい情報を含むものを復号することなく特定する技術は、検索可能暗号化方式(Searchable Encryption)と呼ばれており、いくつかの方式が提案されている。従来方式に共通するのは、検索を行う主体に対して最後まで平文が開示されないという点である。これに対して研究代表者は「検索及び部分開示可能な暗号化方式」に関する研究を進めてきた。この手法では、暗号化された複数のデータについて、ある条件を満たすか否かを、データを復号化することなく判定し、かつ条件を満たすデータだけを復号化し開示することを可能とするものである。

２．研究の目的

本研究の目的は、情報の開示範囲を制御できる機構を有する監査用暗号ログの記録方式を、P2P ネットワークを利用した分散記録方式に拡張することで、P2P 上にロバストなログストレージを構成するために必要な技術開発を行うことである。具体的には、以下の 2 つである。

(1) P2P のノードに対して情報が漏れないことを担保すること。
　本研究では、分散配置されたログのメッセージは、P2P ネットワークのノード、すなわち他人の PC 上に保存されることを想定している。このとき、各ノードがプロトコルを遵守する保証がない。このような状況においても安全性が保たれることを示さなければならない。

(2) 実際にプロトタイプ上に実装を行うことで、提案手法である P2P ネットワークを利用した監査ログシステムの実現可能性を確認すること。

(3) 検索可能暗号化方式の検索条件の柔軟化。
　検索可能暗号化では、特定のキーワードをタグ付けしたものを検索する方式が多く、平文での検索のような部分一致検索や AND/OR 検索といったことが難しい。部分開示の条件の下で、検索条件の柔軟化・多様化を目指す。

３．研究の方法

P2P に基づくログストレージは、分散ファイルシステムの上に対改ざん性を持つログストレージを構成することで実現される。ログメッセージは、暗号化されて分散保管され、ログの閲覧時には検索可能暗号化による。

検索可能暗号方式は、一般的に、開示用の暗号データと、検索時に使用する照合用データから構成される。特に、検索主体に対して情報が漏れるかどうかは、この照合用データの構成方法に左右される。本研究では、情報が漏えいしないことの理論的な裏付けを得るとともに、その方式の実装を行う。

実装は、4 台のノート PC を用いた小規模なネットワークを構築し、各 PC で生成されたログメッセージを残り 3 台の PC に分散配置するシステムを構築する。実装は、保持すべきデータ量や処理速度を無視した原理的な試作と、実用を視野に入れた高速化の段階を考える。

実用的な速度での稼働が見込めるようであれば、ネットワークシミュレータ上でより多くの PC が接続されたネットワーク環境をシミュレートすることで、ログストレージ全体の特性を評価する計画であった。

４．研究成果

(1) 従来、検索可能暗号方式における安全性の証明では、メッセージを保持するサーバは Honest but Curious、すなわち情報を不正に得ようとはするが、検索可能暗号化方式の処理手順（プロトコル）自体は遵守することが前提とされていた。しかし、本研究ではログメッセージを蓄積するのは P2P ネットワークのノードであるため、ノードがプロトコルを遵守する保証がない。このような状況においても安全性が保たれることを示さなければならないことが判明した。
　本研究で考えている方式では、オリジナルのログメッセージは、秘密分散法を用いて複数のシェアに分割され、各シェアが P2P 上のノードに格納される。問い合わせの際に、保管したシェアを正しく取り出すことができなければ、オリジナルのログメッセージを再構築することができないこととなる。
　そこでノードがプロトコルを遵守しない前提でも安全性を確保できるかどうか

を理論的に検証することとした。まず暗号化されたログメッセージを生成するノードをクライアント、メッセージを保存するノードをサーバとみたてた。すなわち、一般のサーバクライアント型の検索可能暗号化方式としてモデル化を行った上で、サーバが不正な処理を行った場合に、クライアントが検出できる方式を提案した。本手法では、サーバに保管する照合用データおよび開示用データの双方について、メッセージ認証コードによる検証情報を付加することにより、サーバから送り返された値の正当性を検証する。本手法は Universal Composability の元で安全性が証明されているため、他の暗号プロトコルの部品として使用しても安全性が揺らぐことはない。

(2) プロトタイプシステムの実装
4 台の PC を相互にネットワークで接続し、それぞれの PC で生成されるメッセージを残り 3 台の上に分散記録するプロトタイプの作成を行った。このプロトタイプは原理の確認であり、通信コストや計算コストは考慮しないこととした。通信部分の実装を簡略化するために、ログシステムとしての通信プロトコルは HTTP 上に実装した。また各ノード上のプロセスは、CGI プログラムとして実装した。動作速度は非常に遅かったが、ログメッセージが各ノードに分散記録され、また条件に一致するメッセージを取得できることを確認した。

(3) 動的更新に対する安全性の保証
(1)での安全性の証明では、クライアントがサーバに開示情報や照合用情報を保管したあと、それらが変更されないことが前提となっていた。しかしログストレージを構成する場合、ノードには次々と新しいログメッセージが追加記録されていくことになる。すなわち開示用データや照合用データが更新されていくことになる。
データの更新を認める場合には、(1)で開発した手法では、サーバの不正を検出できないケースがあることが判った。具体的には、データの更新を行った時に、サーバが古いデータを送り返す「リプレイアタック」を検出することができないことがわかった。そこで、データの追加・更新・削除が行われる場合でも、サーバの不正を検出できる方式を新たに開発した。
本手法では、照合用データ及び開示用データの最新の状態を、検証用の一つの値 A に集約して表す。クライアントは、データの更新に伴って、この値がどのように変化するか計算することができる。サーバは検索結果をクライアントに返送するにあたって、サーバが保持している最新の照合用データと開示用データに音づいて、検証用の値 B を計算する。クライアントは、この検証用の値 B、検索結果、検証用の値 A との間の整合性を検証することで、サーバが最新の値を返送して来たのかを判定することができる。

(4) プロトタイプシステムの実装 2
ノードの不正行為対策を厳密に確保するために、(3)の検出手法をプロトタイプ上に実装を試みた。検証の値 A を求める方式としては RSA Accumulator という手法を使用している。この手法は、データの更新時および検索時にサーバ上の計算コストが非常に大きくなるという欠点がある。実際、プロトタイプを動作させたところ、各ノードがそれぞれ新しいログメッセージを一つ生成する度に、全体としては 4 メッセージ×3 ノードのデータ更新が生じることとなり、非常に負荷が高いものとなった。
実効性を確認するために、提案手法をネイティブプログラムとして実装してみたが、効率よく動作させるには至らなかった。

以上の結果から、P2P の各ノードに対して、情報を漏洩しないように、かつ、各ノードが正しく処理を実行していることを検証できる枠組みを提案することはできたものの、実効性の面からはまだ改良の必要があることが判った。

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）

〔学会発表〕（計 2 件）

(1) Kaoru Kurosawa and Yasuhiro Ohtaki, How to Update Documents Verifiably in Searchable Symmetric Encryption, The 12th International Conference on Cryptology and Network Security. Lecture Notes in Computer Science Vol.8257, pp309-328,査読有, 2013.11.21, Paraty, Brazil.

(2) Kaoru Kurosawa and Yasuhiro Ohtaki, UC-secure searchable symmetric encryption, International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science Vol.7397, pp.285-298, 査読有, 2012.3.1 Bonaire.

〔産業財産権〕
○出願状況（計 2 件）

名称：検索システム、検索方法および検索プログラム
発明者：黒澤馨、大瀧保広
権利者：茨城大学
種類：特許
番号：特願 2013-45246
出願年月日：2013/03/07
国内外の別：国内

名称：検索システム、検索方法および検索プログラム
発明者：黒澤馨、大瀧保広
権利者：茨城大学
種類： 特許
番号：特願 2012−20691
出願年月日：2012/02/02
国内外の別：国内

〔その他〕
無し

６．研究組織
(1)研究代表者
大瀧　保広（YASUHIRO OHTAKI）
茨城大学・IT 基盤センター・准教授
研究者番号：３０２６１７３８

(2)研究分担者
無し

(3)連携研究者
無し

(4)研究協力者
無し