様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １６ 日現在

機関番号：１２１０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２８９

研究課題名（和文）検索可能暗号の応用システムに関する研究

研究課題名（英文）Research on application systems of searchable encryption

研究代表者
大瀧　保広（Ohtaki, Yasuhiro）

茨城大学・情報戦略機構・教授

研究者番号：３０２６１７３８

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：検索可能暗号技術はデータを暗号化して記録し、それらを復号することなく特定のキーワードを含むデータを特定する技術である。検索のためにキーワードとそれを含むデータとの対応関係を暗号化インデックスとして構成する。暗号化インデックスの実装方法として、主記憶上で配列や各種ハッシュを用いた方法、二次記憶を用いる方法としてファイルやDBなどを用いた方法がある。テスト用のデータセットを作成した上で、これら各種方式について速度や耐故障性などの観点から評価を行った。実システムを構築する際にはDBを利用することが必須であり、インデックス操作における問題点は要素技術の問題に帰着できることがわかった。

研究成果の学術的意義や社会的意義
現在多くの情報システムがクラウド上に展開されており、多くの場合データベースを利用している。社会的意義として、これらの情報システムの一部に検索可能暗号を適用した部分が自然に追加実装することが可能であるといえる。また学術的には、検索可能暗号方式の提案が数学的モデルでの提案のみであったとしても、実際には実装不能であるといった問題が生じる恐れは低いことがわかった。

研究成果の概要（英文）：Searchable encryption is a technique that records various data in encrypted form and identifies data containing specific keywords without decrypting them. In searchable encryption, the correspondence between keywords and the data containing them is constructed as an encrypted index. The purpose of this study is to clarify the issues involved in implementing a encrypted index.
After creating a data set for testing, we evaluated these various schemes in terms of speed, fault-tolerance, and so on. As a result, it was found that most of the problems in implementing searchable encryption can be turned into problems of elemental technology, and that no major problems arise in constructing the actual system.

研究分野：暗号応用システム

キーワード：検索可能暗号　実装技術　応用情報システム

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様式Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1)クラウドサービスが普及するにつれて、これまで組織内に設置されたサーバで行なっていた処理をクラウドサーバで実行することが増えつつある。このとき顧客の個人情報など、組織にとっての機微な情報が取り扱われることもある。万が一の情報漏洩の危険性を小さくする技術として秘匿計算や検索可能暗号などが注目されている。

(2)検索可能暗号技術とは、様々なデータを暗号化した状態で記録し、それらを復号することなく特定のキーワードを含むデータを特定できるものである。一般的な検索可能暗号技術では、キーワードとそれを含むデータとの対応関係を「暗号化インデックス」として構成し、これを利用して検索を行う。動的な検索可能暗号では暗号化ドキュメントと暗号化インデックスを一度格納した後に、ドキュメントの追加・更新・削除が行える。

(3)様々な動的な検索可能暗号技術が提案されているが、一般に機能の追加と安全性の証明が中心的な話題である。そのため、数学的なモデルでの提案だけで実装まで行っていないものも多く、具体的な実装にまで触れられているものは少ない。

２．研究の目的

(1)検索可能暗号技術を応用した情報システムを構築する際には、暗号化インデックスをいかに実装するかが重要な問題となる。特に数学的モデルとしてのみ提案された暗号化インデックスを実際にプログラムとして実現しようとすると様々な問題点が想定される。本研究では実システムとしての運用を前提に、暗号化インデックスのデータ構造とその操作手順の実現時における問題点を解明する。

(2)どのような点が実装上の問題点となるかが明らかに判明したら、それらの問題点を解決するための方法を明らかにする。

３．研究の方法

仮想基盤上にサーバ環境を用意し、以下の順にステップごとに実現方法の問題点について検討を行った。

(1) データ構造と操作手順の実現方法の問題点の解明

まず初めに様々な検索可能暗号方式の提案手法について「動作検証レベルの実装における問題点」を扱う。これは提案手法の実現可能性の確認に相当する。暗号化インデックスは主記憶上のデータ構造として実現される。基本的な検索可能暗号のモデルを実際に実装し、必要となる要素技術の確認を行う。

(2) システムとしての実装方法における問題点の解明

次に実際の応用システムを構築する際に生じる実装上の問題点を扱う。実応用システムに検索可能暗号技術を組み込んだ場合、暗号化インデックスはクライアントからサーバに送信される必要があり、さらに暗号化された文書とともにファイルサーバ上に保存される必要がある。システムの再起動などがあっても暗号化インデックスが継続的に運用される必要がでてくることから、暗号化インデックスのデータ構造および操作方法をファイルやデータベースに格納する形へと具体化することになる。

(3) 分散システム上での実装における問題点の解明

クラウドサーバでは、サービスの安定稼働や物理的な資源量の制約を破るために、データの冗長化や分散化などが日常的に行われている。したがって、検索可能暗号を利用したシステムも、複数サーバ上に分散構築されることを想定すべきである。このときデータを分散配置するだけでなく、暗号化インデックス自体も複数サーバ上に分散配置することとなる。分散システム上での暗号化インデックスの実装特有の問題点がないか確認する。

４．研究成果

(1)数学的な提案モデルでは通常単なる表として表現されることが多い暗号化インデックスのデータ構造について検討を行った。想定される実装上の問題点としては、表のサイズの管理方法、可変長であることが求められる文書リストの格納方法、高速な検索の実現方法などが考えられる。そこで、暗号化インデックスの典型的なデータ構造として線形リストとマトリックスを用いる方式の 2 種類について、オンメモリ上に単純配列、単純ハッシュ、Hopscotch ハッシュなどによる実装を行った。Hopscotch ハッシュはデータの削除にも対応できるハッシュテーブルである。評価用データを用いた評価実験を行い、メモリが枯渇しない範囲内において問題なく動作することが確認された。

(2) 実システムの運用継続性を考えた場合には、(1)で取り上げたようなデータ構造をファイルシステムやデータベース上の表現への落とし込みが必要となる。線形リストを用いる方法ではポインタをどのように表現するか、またマトリックスをベースとする方式ではデータの増加に伴うマトリックスサイズの変化に対応する格納方法などが実装上の問題となることがわかった。特にファイルではバイトストリームとなるため、複数の表、木構造、グラフ構造をもつ暗号化インデックスをシリアル化して格納してしまうとアクセス効率が極端に低下するだけでなく、暗号化インデックスの更新が難しい。データベースを利用した暗号化インデックスの実装として、リレーショナルデータベースである MariaDB と NoSQL データベースである(MongoDB と Redis)での実装を行った。NoSQL データベースとは非構造化データの格納に柔軟に対応できるデータベースである。

さらに実応用システムへの適用を念頭に DNS のクエリとレスポンスのログを格納する検索システムを構築した。評価用のテストデータを用いて格納と検索に要する計算量の評価を行った結果、単純にモデルに沿って実装しただけでは実運用に耐える処理速度が達成できないことがわかった。一方で、トランザクション上の問題、ストレージ枯渇時の問題は、検索可能暗号に限らず通常のデータベースの問題に帰着することが可能であることが確認された。

(4)分散システムにおける暗号化インデックスの実装は、実システムを考えた場合には暗号化インデックスのところで分散するのではなく、基盤となるデータベースとして分散データベースを利用すれば十分であることが確認された。当初はファイルシステム上に直接インデックスを構築することが望ましいと思われたが、保守性や堅牢性の観点からはデータベース上に構築したほうが望ましい。なお処理時間についてはデータベースの特徴を踏まえて実装することが重要である。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Ohtaki Yasuhiro、Togashi Kenta	４．巻 1264
２．論文標題 A Practical Implementation of Searchable Encrypted Audit Logging System	５．発行年 2020年
３．雑誌名 Advances in Networked-Based Information Systems. NBiS 2020. Advances in Intelligent Systems and Computing,	６．最初と最後の頁 549～559
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57811-4_55	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関