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　　元 年　　６ 月 ２０ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１４９

研究課題名（和文）クラウド環境におけるセキュアなデータ販売市場支援システム

研究課題名（英文）Secure data market support system in cloud environment

研究代表者
渡辺　知恵美（Watanabe, Chiemi）

筑波大学・図書館情報メディア系・准教授

研究者番号：２０３６２８３２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究ではクラウドにおけるセキュアなデータ販売市場支援システムについての研究を行った。資産であるデータをクラウド上での安全性を確保するために暗号技術を用いたデータ管理手法を提案した．索引をクライアントとサーバに分割することで安全かつ高速な検索を実現した．問合せによるデータ販売を行うために、クライアントが問合せによって獲得した情報を定量化する関係式を考案した．また資産としてのデータ販売をブロックチェーン上で行うためのプロトコルを提案し実装した．

研究成果の学術的意義や社会的意義
データの資産としての価値が重視され、データの公開に関して慎重な処理が求められる今日において暗号化によるデータ販売の重要性は日に日に高まっている。本研究は暗号化データベースを応用したデータ販売の基盤システムに関する基礎研究であり、高速な検索スキーム・利用者の獲得情報の定量化・ブロックチェーンにおけるセキュアな資産売買の基盤システムについて提案を行っている。今後の実用化における価値は非常に高いと言える。

研究成果の概要（英文）：In this study, we researched a secure data market support system in the cloud. First, we proposed a data management method using cryptographic technology in order to ensure the security of confidential data on the cloud. We proposed and achieved a safe and fast query scheme by dividing the index into client and server. In addition, for selling the data, we have defined an expression that quantifies the information the client acquired by the queries. We also proposed and implemented a protocol for selling data as assets on a block chain.

研究分野：データベースシステム

キーワード：暗号化データベース　セキュリティ　データ販売　クラウド環境　データベース

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

ビッグデータの利活用による企業のサービス品質向上および新たな販売戦略立案の重要性に注目が集まっている。地理データや地理に結び付けられたユーザの行動データ（Google Map）、Facebook や Twitter 等のソーシャルデータ、 企業状況データ（Dan & Bradstreet）など様々なデータは一般社会における人々の行動や動向などを反映し、これらの分析結果の利用がマーケティングでの主導権を握る社会となりつつある。それに伴い分析のためのデータに対する市場価値が高まり、データを販売するデータマーケティングはますます重要となりつつある。Scholem らの報告では現在 46 以上のデータサプライヤがおり、Dun & Bradstreet や Reuters 等でも Web 上でのデータ販売を開始している。

上記の環境においてデータは重要な資産である。データ管理や受け渡しには慎重な取り決めが必要となり、データ市場のための安全で強固なデータ管理および販売環境が必須である。最新のデータを利用者に提供するにはファイル単位によるデータ販売より API によるデータ提供が適切であると言える。API を用いることでデータ利用を制限したり利用履歴を管理できるという利点もある。しかしながらデータ所有者・販売者自らがデータ管理・販売および API 等の整備を行うには大きなコストがかかる。

２．研究の目的

本研究ではこのようなクラウドにおけるデータ販売市場支援システムについての研究を行った。特に資産であるデータをクラウド上での安全性を確保するために暗号技術を用いたデータ管理手法を提案した。データ所有者は管理および販売やデータの受け渡し等をクラウド上のサービスプロバイダに委託する。 またデータの販売契約を利用者と交わす。提案するシステムではデータを API で提供することを想定する。契約を締結した利用者はデータを取得する権限を持ち、 API を通して必要なデータを問合せ、 データを取得する。クラウド上のサービスはデータ販売契約やデータの管理、API を通した問合せ応答を行い、 サービスプロバイダはこのサービスの管理者として運用を行う。

３．研究の方法

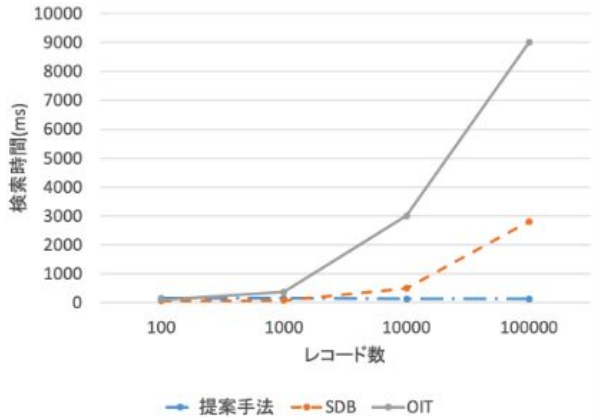
我々は以下の項目に分け研究を進めた

1. 大規模データに対する暗号化索引を利用した安全かつ高速な演算フレームワークを開発する。
2. データ販売契約に基づくアクセス制限機構: データ市場動向や DataEco$y$tem 等で用いられているデータ販売契約について調査し、それらの契約に基づいた API 利用のアクセス制限機構およびアクセス監視手法を提案し検証する。
3. 安全なデータ更新手法:データの更新・削除・挿入は索引の更新を伴うためデータ内容の推測につながる。更新内容をサービスプロバイダから秘匿する安全な手法を提案し検証する。

４．研究成果

研究項目１に関して、安全かつ高速な演算フレームワークを提案し、開発した。検索高速化のためには索引を使うのが一般的であるが索引の構造や検索時の探索パターンにより元データを推測される恐れがある。そのため、本研究ではサーバ上で索引の構造を秘匿した索引による検索手法を提案した。通常の索引はノード間の順序関係により値の大小関係が推測できる問題がある。しかし本研究において索引はサーバに格納されているが、ノード間の順序関係を保持していないため構造から内容を推測されにくい。また、クエリに対してもノイズを付与するこ

とで、索引へのアクセス頻度をもとに値を推測されないことを保証した。本索引を用いて実現可能なクエリは、属性の選択演算で、完全一致と範囲検索、文字列属性の部分一致など基本的な演算スキームを提供した。本提案手法における検索時間を既存手法と比較した結果を示す。既存手法はレコード数に対して指数的に検索時間が経過する傾向にあるが、本提案手法は 10 万レコードに対しても 100ms 以下の検索時間にとどめた。一回のクエリで 10 回程度のインタラクションが必要となるが、1 回の通信データ量が少ないため、サーバで各レコードに対して条件を満たすかどうかチェックするタイプの検索と比較して大幅に検索時間が短縮された。



研究項目 2 に関しては、研究項目 1 にて開発したシステムにおいて、クライアントが問い合わせによって獲得した情報を、 エントロピーを用いて定量的に評価する手法を提案した。またデータ提供サービスのモデルを考案した。提案した定量化のための計算をデータ所有者、クライアント、サービスプロバイダの誰が行うのか検討し、定量化した値を基にクライアントが持つ検索権の範囲内で問合せを行うことができるデータ提供サービスのモデルを設計した。ただし本項目においては、クライアントの得た情報に関する基礎的な定量化に止まり、実際のデータの価格設定等はデータ販売の経済的な観点での分析や設計を十分に行うことができず、計画通りには進めることができなかった。

データ販売プラットホームの整備においては、クラウド上でのサーバを用いたサーバ・クライアント形式のアーキテクチャを想定しているが、そのほかにブロックチェーン型システムにおいても実現するべきと考え、データを秘匿化した状態での資産売買スキームを提案し実装した。プロトコルでは、取引者間でのメタ的な契約に関する合意をした後に、所定の支払いを行っていく 2 フェーズで構成し、その一貫性を保証した。また、利息を考慮した分割払いにも対応した。安全性評価では、ケースごとにプロトコルの安全性を示した。評価実験では、範囲証明の実行時間及び証明サイズを計測し、処理時間に関してはボトルネックとなり得ないことを示した。これに加えて、送金トランザクション発行の処理速度が 1.0 秒以内であることを測定し、実用的であることを検証した。仮想通貨のような数 ms のようなリアルタイムトランザクションへの対応は難しいが、不動産の資産売買など数秒単位のリアルタイムなトランザクションであれば十分に実現可能であることがわかった。

研究項目 3 においては、データの更新はデータ内容の推測につながるため非常にチャレンジングな問題であり、取り組む価値の高い項目であったが期間中の手法の提案には至らなかったための今後の課題として取り組んでいきたいと考えている。

５．主な発表論文等

〔雑誌論文〕（計 2 件）

1. 秋山賢人，渡辺知恵美，天笠俊之，北川博之:暗号化データベースにおける構造と

データを分離した索引を用いた安全かつ高速な検索手法，情報処理学会論文誌データベース（TOD81），Vol. 12, No. 2, pp. 1-11, 2019
2. 秋山賢人，渡辺知恵美，北川博之: 暗号化データベースシステムにおけるクエリベースのデータ販売スキーム．情報処理学会論文誌データベース (TOD76) , Vol. 10, No. 4, pp.31 - 35, 2017

〔学会発表〕（計 9 件）
1. 安坂祐紀，渡辺知恵美，天笠俊之，北川博之:取引額を秘匿したブロックチェーンにおける取引者間合意による資産売買プロトコル，第 11 回データ工学と情報マネジメントに関するフォーラム (DEIM 2019), I6-4 , 2019.
2. 安坂祐紀，渡辺知恵美，天笠俊之，北川博之: プライバシーを考慮したブロックチェーンの取引者間事前合意プロトコル，コンピュータセキュリティシンポジウム, 3B3-2, 2018.
3. 秋山賢人，渡辺知恵美，北川博之: 秘匿検索フレームワーク OSIT を利用したデータ提供サービス，第 10 回データ工学と情報マネジメントに関するフォーラム (DEIM 2018), F7-1, 2018.
4. Kento Akiyama, Chisato Shinozuka, Chiemi Watanabe, Toshiyuki Amagasa and Hiroyuki Kitagawa: An Index-based Secure Query Processing Scheme for Outsourced Databases. The 19th International Conference on Information Integration and Web-based Applications and Services (iiWAS2017), 2017; 224 - 233
5. Mateus S. H. Cruz, Toshiyuki Amagasa, Chiemi Watanabe, Wenjie Lu and Hiroyuki Kitagawa: Secure Similarity Joins Using Fully Homomorphic Encryption. The 19th International Conference on Information Integration and Web-based Applications and Services (iiWAS2017), 2017; 215 - 223
6. 秋山賢人，渡辺知恵美，北川博之: 暗号化データベースシステムにおけるクエリベースのデータ販売スキーム，第 10 回 Web とデータベースに関するフォーラム（WebDBForum2017），2017.
7. 篠塚 千愛，渡辺 知恵美，北川 博之，:暗号化データベースにおけるデータの秘匿性を保証した検索手法，第 9 回データ工学と情報マネジメントに関するフォーラム (DEIM 2017), H6-4 , 2017.
8. 秋山 賢人，渡辺 知恵美，北川 博之: 秘匿検索フレームワーク OSIT における最適なクエリプラン選択法，第 9 回データ工学と情報マネジメントに関するフォーラム (DEIM 2017) , H6-5 , 2017.
9. 合田 真也，渡辺 知恵美，北川 博之: CryptDB の処理時間分析と高速化案,情報処理学会研究報告データベースシステム（DBS） (2017-DBS-164(8)), 2017.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕

６．研究組織
(1)研究分担者 なし
(2)研究協力者
研究協力者氏名：北川博之
ローマ字氏名：Hiroyuki Kitagawa
研究協力者氏名：天笠俊之
ローマ字氏名：Toshiyuki Amagasa
研究協力者氏名：佐久間淳
ローマ字氏名：Jun Sakuma