氏　　名	趙　方明		
学位の種類	博　士（　工学　）		
学位記番号	博　甲　第　8067　号		
学位授与年月日	平成　29 年　3 月　24 日		
学位授与の要件	学位規則第４条第１項該当		
審査研究科	システム情報工学研究科		
学位論文題目	A Study on Cryptographic Cloud Storage with Secure Keyword Search（暗号化クラウドストレージにおける安全なキーワード検索方式の研究）		
主　　査	筑波大学　准教授	博士（工学）	西出　隆志
副　　査	筑波大学　名誉教授	工学博士	岡本　栄司
副　　査	筑波大学　教授	博士（工学）	佐久間　淳
副　　査	筑波大学　准教授	工学博士	片岸　一起
副　　査	筑波大学　准教授	博士（情報科学）	面　和成

論　文　の　要　旨

本論文では、暗号化クラウドストレージに保存されているデータを安全に利用するためのアクセス制御と秘匿検索方式に関する研究について述べられている。

最初にどこからでも計算資源やストレージ資源へのアクセスを可能とするサービスの利便性と、暗号化技術に基づくデータ安全性を両立させる「暗号化クラウドストレージ」の研究背景、関連研究、研究動機と貢献について述べられている。

そして、暗号化クラウドストレージの最先端利用形態における 2 つのキーとなる技術、暗号技術に基づくアクセス制御および秘匿検索方式をサーベイし、既存研究の問題点が論じられている。

次に、シングルユーザが利用する暗号化クラウドストレージの利用形態において、より柔軟な検索条件の指定が可能となるようワイルドカード利用を許した秘匿類似検索方式が提案されている。検索利便性の向上を目指して、クラウドストレージにある暗号文データに対し、より自由かつ実用的な検索機能が求められているが、提案方式では複数文字を柔軟に表現できるワイルドカード指定検索を、ブルームフィルタと呼ばれるデータ構造を上手く利用することで実現している。その結果、従来の完全一致検索やシングル文字ワイルドカードによる検索に比べ、秘匿検索が対応できる文字列表現の範囲を拡張することに成功している。また、クラウドサーバ側に置く検索照合用のインデックスに高速なハッシュ関数ベースのマスクをつけ、インデックスからクラウドサーバへの余分な情報漏洩を防止しつつ、検索実行時にクラウド側の計算資源を有効に利用することで、検索者側の負荷軽減も達成している。

更に、複数ユーザが利用する暗号化クラウドストレージの特徴を分析し、クラウドに保存されている暗号化データに対し、ユーザらが様々なアクセス権限(新規作成，読み取り，書き込み，キーワー

キーワード検索)を持つという点を考慮し、属性暗号技術に基づく複数ユーザ対応の暗号データ共有方式と秘匿検索方式を提案している。大量の暗号データと所有アクセス権限が異なるユーザらが共存する環境において、属性ツリーを用いた暗号データへの柔軟なアクセス制御を実現すると共に、検索者のアクセス制御権限を考慮した秘匿検索方式を提案している。検索時にクラウドサーバは検索者の復号できるファイル群に絞り込んで検索を行うことで、アクセス権限を考慮しない既存の暗号文検索手法における検索効率と情報漏洩の問題点を解決し、提案方式の既存手法に対する優位性を示している。また、性能評価とシミュレーションにより、提案手法の有効性も明らかにしている。

審　査　の　要　旨

【批評】

クラウドストレージサービスでは、データを外部サーバに置くというアウトソーシングの形態を取ることから、クラウド業者を必ずしも完全に信頼できないという前提でデータの秘匿性に関する問題を解決することが望まれている。クラウドに置く前にデータを暗号化することで安全性を得ることができるが、それと同時に、利用者が指定したキーワードに対する柔軟な検索の実現や，複数ユーザが共有する暗号データに対する適切なアクセス制御の実現が重要な課題となる。

本論文では、暗号化クラウドストレージにおける情報漏洩を防止する秘匿検索手法と柔軟なアクセス制御手法に関する研究について述べている。まず、シングルユーザが利用する暗号化クラウドストレージ環境において、ブルームフィルタのデータ構造を用いたワイルドカード指定可能な秘匿類似検索方式を提案している。提案方式では複数文字を表現するワイルドカードを含む検索条件をブルームフィルタに変換して秘匿検索に利用し、そして効率的に検索インデックスを秘匿するマスクをつけることによって、類似検索機能を達成しながらクラウドサーバへの情報漏洩を抑制している。このブルームフィルタへの変換の際には特殊なエンコーディングを用いることで、処理効率が多項式時間に収まるよう工夫している。

また、複数ユーザが利用する暗号化クラウドストレージの特徴を考慮し、暗号データに対してユーザらが持つアクセス権限を活用し、属性暗号技術を用いた複数ユーザ対応の暗号データ共有方式と秘匿検索方式を提案している。これは、属性ツリーを用いた暗号データへの柔軟なアクセス制御を実現すると共に、検索者のアクセス権限を考慮に入れた秘匿検索方式を初めて提案している。既存研究の問題であった検索効率と検索結果からの余分な情報漏洩という問題を、検索時にクラウドサーバが検索者の復号できるファイル群のみに検索をかけることで回避しており、実用的観点から有用であると考えられる。さらに性能評価とシミュレーションの結果によって提案手法の有効性を明らかにしていることも評価できる。

以上、本論文は、暗号化クラウドストレージにおけるセキュリティ課題を解決する有用な秘匿検索方式とアクセス制御方式を提案しており、博士論文として十分な価値を有するものと認められる。

【最終試験の結果】

平成 29 年 2 月 9 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。この結果とリスク工学専攻における達成度評価による結果に基づき、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。