（博甲）

氏　　名	須賀　祐治
学位の種類	博　士（　工学　）
学位記番号	博　甲　第　7695　号
学位授与年月日	平成　28 年　3 月　25 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	クラウド環境におけるデータ委託と外部操作に適した秘密分散方式の研究

主　　査	筑波大学　教授	工学博士	岡本　栄司
副　　査	筑波大学　教授	博士(工学)	古賀　弘樹
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(工学)	西出　隆志
副　　査	筑波大学　助教	博士(理学)	金山　直樹

論　文　の　要　旨

本論文では、クラウドシステムのセキュリティを扱っているが、まず最初に、セキュリティの３要素となる秘匿性、完全性、可用性の確保の重要性を実例を引用しつつ述べている。

そして、そのような状況で使える仕組みとして、秘密情報分散方式を取り上げている。まずデータに対する秘密分散方式として分散・復元時に排他的論理和だけを用いて構成する秘密分散法(XOR-SSS) の新しい構成方式を提案している。クラウド環境では大量のデータを扱うためにより高速な処理が求められるが、提案方式は排他的論理和だけを用いるため、従来構成法に比べてはるかに高速に分散・復元が可能であるという優位性を持つ。また、オリジナルとシェアのサイズが不変な秘密分散法でもあり、ストレージを有効に使う意味でもクラウドへの適合性が高い。さらに、データは秘匿性確保のため暗号化されることも多いが、データ処理をクラウド上で行う際に復号しなくてもよいように、XOR-SSS では秘密分散化と暗号化が可換となっている。

次に、クラウド上にアクセスするための認証方式への応用として、復号に計算リソースを必要としない視覚復号型秘密分散法(VSSS)を提案している。そして、実情にあった使い方ができるように、従来のグラフタイプ視覚復号型秘密分散法(GVSSS)を改良して、復元するための権限間に柔軟に差をつけられるようにしている。

最後に、提案したXOR-SSSとGVSSSを組み合わせた例を構築し、セキュリティの３要件である秘匿性、完全性、可用性をトータルでカバーできることを示している。

審　査　の　要　旨

【批評】

クラウドシステムの普及に伴って、セキュリティの確保が重要な課題になってきている。特に信頼性、プライバシについてはユーザの要求が高いため、クラウド業者は信頼できないという前提でシステムを構成する必要がある。

そのような状況で有用な方式として、本論文では、秘密情報分散方式を取り上げているが、従来からこれが有力であることは認識されていた。ただ、クラウドには大量のデータがあるため、処理速度、情報拡大率、準同型性の課題があった。

そこで、本論文では、まず、分散・復元時に排他的論理和だけを用いて構成する秘密分散法 (XOR-SSS) の新しい構成方式を提案して、これらの課題を解決している。XOR 主体なので、いずれの課題も比較的簡単にクリアできている。

また、クラウドシステムではアクセスのためのユーザ認証も重要である。そこで、本論文では、それにも秘密情報分散方式の応用を試みているが、ここでは、復号に計算リソースを利用しない視覚復号型秘密分散法 (VSSS) を用いている。確かに大規模システムでは、認証時には計算リソースが少ない方が有利であり、本方式は有力な手法の一つと考えられよう。そして、アクセス権限に差があるような構成ができるようにしている。ただ、一般にVSSSでは画像の量が増えてしまうことが多いため、画像拡大率をできるだけ下げるよう改良を加えている。その議論を進めて、画像拡大率の下限を達成する例を詳しく調べている。これらは今までにない特長であり、極めて有用である。

以上、本論文は、クラウド環境におけるセキュリティの課題を解決する有力な秘密情報分散方式を提案しており、博士論文にふさわしいと認められる。

【最終試験の結果】

平成 28 年 1 月 26 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。