

A Thesis for the Degree of Ph.D. in Engineering

**A Study on Distributed Storage with
Flooding DDoS Attack Detection**

February 2021

Graduate School of Science and Technology
Keio University

Sanghun Choi

Thesis Abstract

No. _____

Registration Number	<input checked="" type="checkbox"/> “KOU” <input type="checkbox"/> “OTSU” No. _____ *Office use only	Name	Sanghun Choi
Thesis Title			
A Study on Distributed Storage with Flooding DDoS Attack Detection			
Thesis Summary <p>Since the owner’s data might be leaked from the centralized server storage, the distributed storage schemes with the server storage have been investigated. However, conventional schemes occur the burden of data capacity and the calculation time for the restoration. In order to overcome these problems, I propose the server-based distributed storage using secret sharing and AES-256 is proposed. However, since the server storage is utilized, when the server storage is attacked by the DDoS attack, the owner data cannot be restored. To keep and restore the owner data from DDoS attack in the proposed server-based distributed storage, I additionally propose the lightweight DDoS attack detection using the bloom filter. I show the effectiveness through data analysis and computer simulation for the distributed storage and DDoS attack detection. The outline of this dissertation is as follows:</p> <p>Chapter 1 deals with the importance of distributed storage and DDoS attack detection. I summarize the fields which this technique is applied. Moreover, I clarify the purpose and role of this dissertation.</p> <p>Chapter 2 deals with the related works of the proposals.</p> <p>Chapter 3 deals with the distributed storage. I propose the server-based distributed storage using secret sharing with AES-256 for lightweight safety restoration. The owner’s data will be safely kept in the distributed storage since all of the divided data are divided into two pieces with the AES-256 and stored in the peer storage and the server storage. Even though the server storage keeps the divided data, the server and the peer storages might know the pair of divided data via Secret Sharing, the owner’s data are secure in the proposed scheme from the inner attack of secret sharing. The evaluations show that the proposed scheme is improved for lightweight, stability, and safety.</p> <p>Chapter 4 deals with the DDoS attack detection. I additionally propose the lightweight detection using bloom filter for the proposed distributed storage. To detect the DDoS attack and ensure the high accuracy, the high true positive rate, and the low false positive rate, the decrement-all operation is used and the checkpoint are flexibly changed depending on the fluctuant packet arrival per second in the bloom filter. The effectiveness is shown by the computer simulation with real dataset.</p> <p>Chapter 5 concludes this dissertation and summarizes the contribution of this work.</p>			

報告番号	㊦ 乙 第 号	氏 名	崔 相勳 チェ サンフン
<p>主論文題名 : A Study on Distributed Storage with Flooding DDoS Attack Detection (Flooding DDoS 攻撃検知を用いた分散ストレージに関する研究)</p>			
<p>(内容の要旨)</p> <p>中央サーバストレージでは、オーナーのデータに問題が発生する可能性があるため、分散ストレージ方式が研究されている。しかし従来の研究では、オーナーのデータを復元するための、演算コストとデータ容量が高いという課題がある。本論文では、その課題を解決するために、Secret sharing と AES(Advanced Encryption Standard)-256 暗号方式を適用した、サーバストレージを使用する分散ストレージ方式や、オーナーのデータを保護するためのサーバストレージに対する DDoS(Distributed Denial of Service) 攻撃を検知する方式を提案し、データ分析や計算機シミュレーションにより、提案方式の有効性を示す。</p> <p>第 1 章では、分散ストレージと DDoS 攻撃検知技術の重要性、および当該技術が用いられる領域を概観し、本研究の目的と位置付けを明確に述べる。</p> <p>第 2 章では、本研究に関連する従来の研究について述べ、その課題点を提示する。</p> <p>第 3 章では、分散ストレージにおける、効果的なオーナーのデータを保護し、演算コストとデータ容量を減らす方式を提案する。オーナーのデータは、Secret sharing と AES-256 によって 2 つに分けられ、サーバストレージとピアストレージにそれぞれ分散保管される。オーナーのデータの一部がサーバストレージへ保管されても、内部攻撃による支障を軽減し、安全性を担保できる。提案方式の有効性を、計算機シミュレーションにより検証し、結果、軽量性、安定性、安全性が、従来方式より改善できることを示す。</p> <p>第 4 章では、3 章で提案した方式への DDoS 攻撃から、オーナーのデータを保護する方式を提案する。オーナーのデータの一部がサーバストレージに保管されているため、内部攻撃による問題発生を防ぐため、Bloom filter を使用する。そして、DDoS 攻撃を検出し、高精度、高真陽性率、および低偽陽性率を確保するために、decrement-all 演算を用いて、秒あたりのパケット到着揺らぎに依存して、判定点を柔軟に変化させる。実データセットを用いた計算機シミュレーションにより、提案方式は検知性能を向上させることが可能であることを示す。</p> <p>第 5 章は結論であり、本論文の内容を総括している。</p>			