複数のパブリッククラウドを組み合わせた安全性向上方式の研究

WAKABAYASHI, Naoki / 若林, 直希

(出版者 / Publisher)
法政大学大学院理工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
59
(開始ページ / Start Page)
1
(終了ページ / End Page)
6
(発行年 / Year)
2018-03-31
(URL)
https://doi.org/10.15002/00021602

複数のパブリッククラウドを組み合わせた安全性向上方式の研究

RESEARCH FOR SAFETY IMPROVEMENT METHOD ON MULTI-CLOUD

若林直希
Naoki WAKABAYASHI
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

Recently, various public cloud services have been popular, and we can use these services at low cost. However, public cloud services have some security issues, for example, an end user can store a file on public cloud services managed by an uncontrollable administrator. Therefore, we propose an approach to solve this security issue for a storage service from the viewpoints of confidentiality and availability by using multiple public services simultaneously. In this paper, we describe how we developed our prototype for multiple actual public service usage and evaluated the performance of our approach. The practicality of our approach is shown.

Key Words *: cloud computing, multi-cloud,secret sharing scheme,availability,confidentiality,*

１．はじめに

近年,クラウドコンピューティングが発展してきたことにより,様々なクラウドサービスが利用されている[1][2][3].その一例として複数のパブリッククラウドを連携して利用することで単一のプライベートクラウドの利用よりも機密性を向上させる方式を提案した.これは一つのファイルを複数のパブリッククラウドに分散し保管することで機密性の向上を実現することができる．また,クライアントが指定する機密性,完全性,可用性のレベルによって複数のクラウドの中から最も適したクラウドの組を選択する.

本論文ではパブリッククラウドストレージサービスを利用することを仮定し,ファイルをクラウドに保存するために,複数のパブリッククラウドの中から最適なクラウドの組を選択し,パブリッククラウドの可用性とコスト面を保ちつつ,機密性と完全性を向上させる方式の提案,プロトタイプの実装を行うことで性能評価を行い,その有能性を示す.

２．前提となる方式

（１）　想定する環境

本提案手法は，複数のクラウドストレージサービスが存在する環境を想定する．また，各クラウドサービスはSLA を公開していることが前提となる．公開されているSLA には本手法で利用する評価項目のすべてが記載されていることが前提とする．更に，クラウドストレージのセキュリティにのみ着目するために，それ以外の要素に基づくセキュリティは確保されているものと考える．そのため，ユーザの端末がコンピュータウィルスに感染していることや，クラウドまでの通信路が盗聴されているといった状況が無いものとして考える.

ユーザは，上述の条件を満たすクラウドサービスと契約済みであり,利用可能な状態であるものとする．また,すべてのストレージサービスは定額課金制であることを前提としている.

（２）　(k,L,n)しきい値秘密分散法

秘密分散法とは，秘密情報と呼ばれる秘密にしたいデータから分散情報と呼ばれる複数のデータを生成し，そのデータをあるしきい値個以上集めることができれば元データを復元することができる符号化技術である(k,n)しきい値秘密分散法[4][5]の拡張手法である．(k,n)しきい値秘密分散法のデメリットである分散情報の肥大化を解決することができる.

ある秘密情報 x に対して(k, L, n)しきい値秘密分散法を適用すると，n 個の分散情報が生成され，そのうち k 個を集めることで秘密情報の復号が可能になる[6] [7]．ここで,各分散情報のデータサイズは秘密情報の 1/L 倍となっている．このとき，k-L 個より多くかつ k 個未満の分散情報からは，秘密情報の一部を特定可能であり，それ以下の個数では情報理論的に安全であり，秘密情報に関する情報を一切得ることができない.

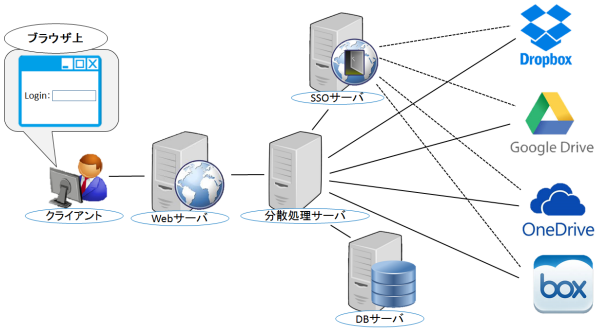
本手法では，この(k，L，n)しきい値秘密分散法をクラウドサービスに保存するデータへ利用する．ユーザがクラウドサービスに預けたいデータを秘密情報として(k, L, n)しきい値秘密分散法を適用する.生成された n 個の分散

情報を，n 個の別々のクラウドサービスに保存しておき，元のデータが必要になった場合にはそのうちの k 個のサービスに接続し，分散情報を得ることで秘密情報が復元可能となる．

３． 提案手法

（１） 全体の構成

本提案手法では，クライアント，Web サーバ，分散処理サーバ，データベースサーバ（DB），SSO サーバ，4 つのクラウドサービス（Dropbox,GoogleDrive,OneDrive,Box）を用いる．今回提案するセキュアなクラウドストレージシステムの全体の構成を図．1 に示す．



図．1 提案手法の全体構成

クライアントは Web サーバと通信をする機能を有する．Web サーバはクライアントが送受信したいデータを分散処理サーバへ送受信する機能を有する．

分散処理サーバは受け取ったデータを AES 方式にて暗号化・復号し，それを秘密分散・復号する機能を有し，各クラウドサービスと DB に情報を保存することができる．さらに，暗号文のハッシュ値と秘密情報復号のための識別情報を生成し，DB に保存する機能も有する．これらの機能を用いてユーザはデータを分散し保存する．

DB サーバはクライアントのアカウント情報，分散処理サーバの生成した各情報を保管する機能を有する．

SSO サーバは，Web アプリケーションのアカウントの認証時に複数のクラウドストレージの認証を行う機能を有する．

本システムの基本的な処理として，秘密情報は秘密分散法により符号化される前に分散処理サーバ上で共通鍵暗号方式により暗号化される．その後，分散処理サーバにて暗号文情報に対して秘密分散法を適用し，分散情報を各クラウドサービスに保存する．また，秘密分散による分散情報からハッシュ値を取得し，復号時に改ざん検知に利用する．

（２） トラストモデル

本システムでは，以下のようなトラストモデルに基づいて安全性を確保する．

クライアントの ID と PW を信頼する．

Web サーバは分散処理サーバとも通信を行うため情報漏洩の危険があり，Web サーバのデータストレージは信頼しない．しかし，Web サーバ上で動作するプログラムは改ざんされないものとする．

分散処理サーバはクライアントから知られていて，クラウドサービスとも通信を行うため情報漏洩の危険があり，分散処理サーバのデータストレージは信頼しない．しかし，分散処理サーバ上で動作するプログラムは改ざんされないものとする．

DB サーバは分散処理サーバから知られていて，仮に分散処理サーバ自身が何らかの情報を持っていた場合に DB サーバに保管され，クライアント側からはクライアントのアカウントにかかわる上だけ取得される可能性があり，DB サーバの情報は改ざんされないものとする．

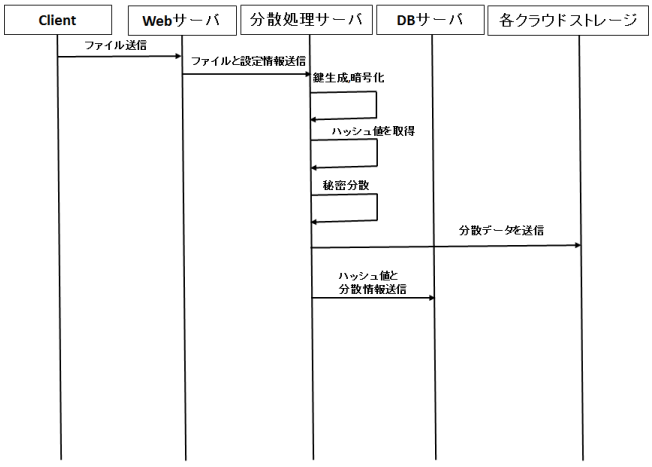
SSO サーバはクライアントの認証時にクライアントが登録しているクラウドを認証する．この時，SSO サーバ上で動作するプログラムは改ざんされないものとする．また，SSO サーバのデータストレージは信頼しない．

クラウドサービスは研究背景で述べた理由により単体でのデータストレージは信頼しない．信頼しないストレージであっても，秘密分散法によって生成された分散データをしきい値未満保管する場合は利用できるものとする．

（３） 分散，復号過程

本システムの具体的な手順をについて述べる．

分散処理時の実行過程の詳細をシーケンス図．2 に示す．



図．2 分散処理時のシーケンス図

分散過程

1．データを保存したいユーザは，Web サーバを通して分散処理サーバに送る．

2．分散処理サーバは共通鍵を用いて暗号化（AES）し，秘密情報にする．

3．秘密情報からハッシュ値を生成する．

4．(k,L,n)しきい値分散法を用いて秘密情報から n 個の分散情報を作成する．

5．分散処理サーバはハッシュ値と秘密分散情報を DB サーバに保管する．
6．分散処理サーバは n 個の分散情報を欠くクラウドストレージに保管する．

復号処理時の実行過程の詳細をシーケンス図.3 に示す．

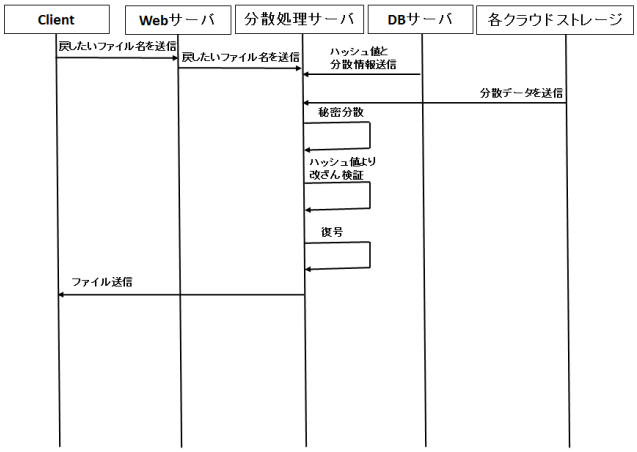


図.3 復号処理時のシーケンス図

復号過程
1．DB サーバにあるハッシュ値と分散情報を分散処理サーバに送信する．
2．分散処理サーバは保管したクラウドストレージサービスを選択肢分散情報をダウンロードする．
3．分散処理サーバは(k,L,n)しきい値秘密分散法を適用して秘密情報を復元する．
4．秘密情報をハッシュ値を用いて検証する．
5．正しければ共通鍵を用いてデータを復号する，正しくなければクライアントに通知．
6．復号したデータをクライアントが受け取る．

4． 実装

本研究では，本提案手法を実環境上でプロトタイプを実装した．クライアントが使用するものとして Web アプリケーションを Web サーバ，分散処理サーバとしてサーバ，DB サーバとしてサーバ，SSO サーバとしてサーバ，クラウドストレージとして一般に利用されている Dropbox,GoogleDrive,OneDrive,Box の 4 つクラウドストレージサービスを用意した．

実装における全体のシステム構成を図. 4 に示す．また各サーバのモジュール構成を図. 5 に示す．

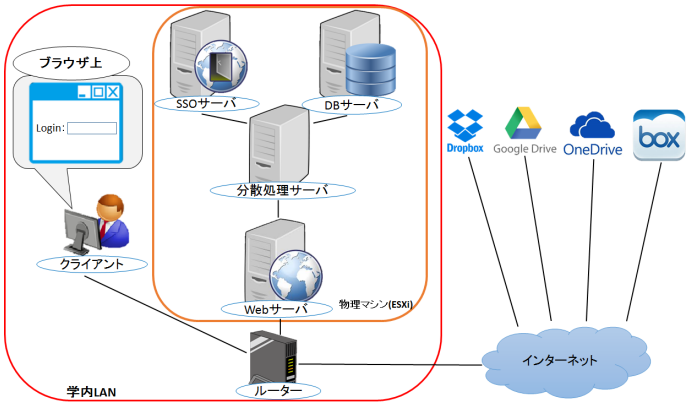


図.4 実装における全体のシステム構成

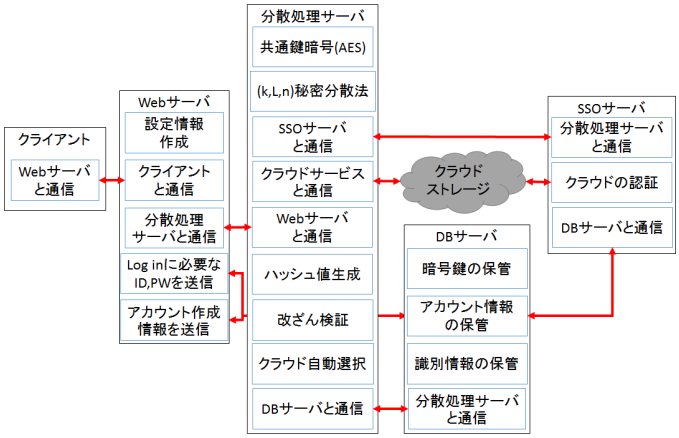


図.5 システムのモジュール構成

クライアントの PC と Web サーバ，分散処理サーバ，DB サーバ，SSO サーバのサーバは学内 LAN で接続され，全てのサーバは物理マシン(ESXi)上に立てている．学内 LAN の途中にルータを設置しルータ経由で通信を行う．またルータからはインターネットに接続され，各クラウドストレージと通信を行う．Web サーバのプログラムはファイルの送受信と各パラメータを分散処理サーバへ送信する機能がある．分散処理サーバのプログラムは Web サーバ，DB サーバ，SSO サーバ，クラウドサービスとの通信，共通鍵の生成，ファイルの共通鍵暗号化・復号，秘密分散による符号化と復号，クラウド選択，メッセージダイジェスト，識別情報の作成などを行う機能がある．DB サーバはアカウント情報の保管，アカウントごとのファイル情報の保管，ハッシュ値の保管，分散ファイルの識別情報の保管する機能がある．また，DB は mysql で構築している．SSO サーバはアカウント認証時にアカウントが登録している全てのクラウドに認証する機能がある．

5． 結果

上述したプロトタイプを用いて，ユーザの要求を元に本提案手法によりクラウドサービスの組み合わせを決定し，(k, L, n) しきい値秘密分散法を用いて実際にパブリッククラウドに分散情報をアップロードした．また，パブリッククラウドから分散情報をダウンロードすることで

元の情報に復号出来ることを確認する．まず初めに，ユーザは要求項目として機密性=2.0，可用性=2.0 を指定し，保存したいファイルである「aaa.txt」を，Web サーバを通して分散処理サーバに送信した．送信した「aaa.txt」を図 6 に示す．分散処理サーバが提案手法により最適なクラウドサービスの組み合わせ k=2, L=1, n=3 のパラメータを使用した時に OneDrive,Dropbox,Box を組み合わせたマルチクラウド環境であるため，これを最適なクラウドサービスの組み合わせとして選出した．これにより，(k，L，n) しきい値秘密分散法を用いて分散情報である「aaa.txt_0.dat」，「aaa.txt_1.dat」及び「aaa.txt_2.dat」を生成し，One Drive，Dropbox，Box の各クラウドサービスにアップロードした．Dropbox へのアップロード結果を図.7，OneDrive へのアップロード結果を図.8，Box へのアップロード結果を図.9 に示す．

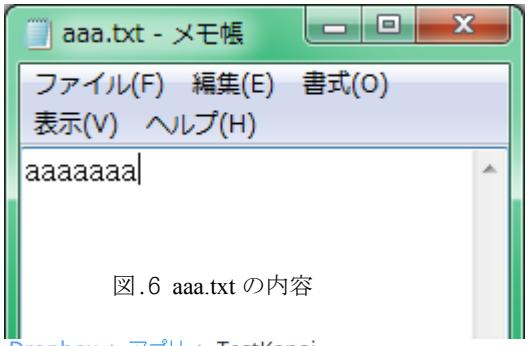


図.6 aaa.txt の内容

図.7 Dropbox へのアップロード結果

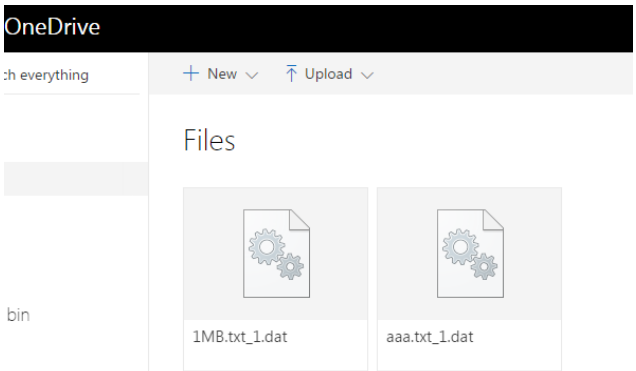


図.8 OneDrive へのアップロード結果

図.9 Box へのアップロード結果

上記でアップロードした「aaa.txt」をダウンロードし

図.10 復号ファイル aaa.txt の内容

以上の結果よりプロトタイプの一連の動作を確認することができた．

６． 評価

実装したシステム評価するためにシステム全体の処理時間と何もデータに手を加えない際の処理時間を比較する．そのときのアップロード時とダウンロード時を図 11, 12 に示す．

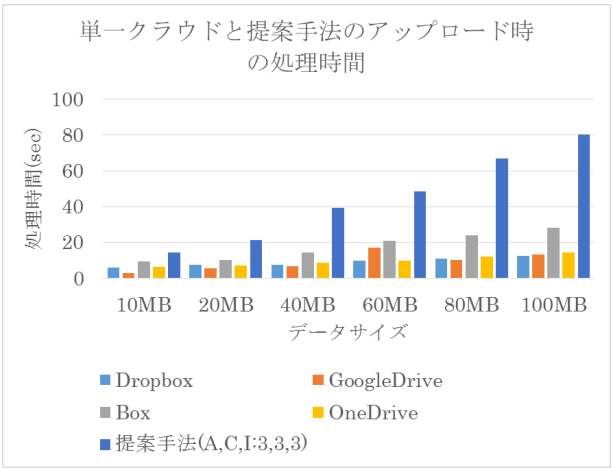


図.11 単一クラウドと提案手法のアップロード時の処理時間

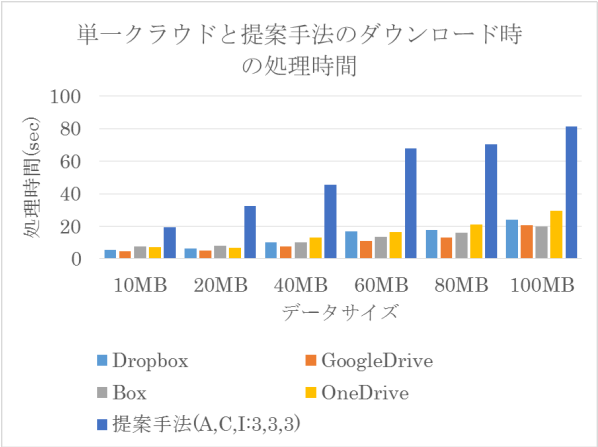


図.12 単一クラウドと提案手法のダウンロード時の処理時間

アップロード,ダウンロード時それぞれで単一クラウドを利用した場合よりも提案手法の方が,処理時間が長いことがわかる.また,容量が増えるにつれて処理時間が長くなることがわかる.単一クラウドよりも処理時間が長いが,大きな差は見られないため十分に実用レベルだといえる.

次に(k,L,n)しきい値秘密分散法のパラメータの関係性について評価する.

パラメータ k,L,n のうち L を 1,n を 5 に固定して k を変化させた場合に提案手法の処理時間がどのように変化するかをファイル容量別に評価した.その結果を図 13,14 に示す.

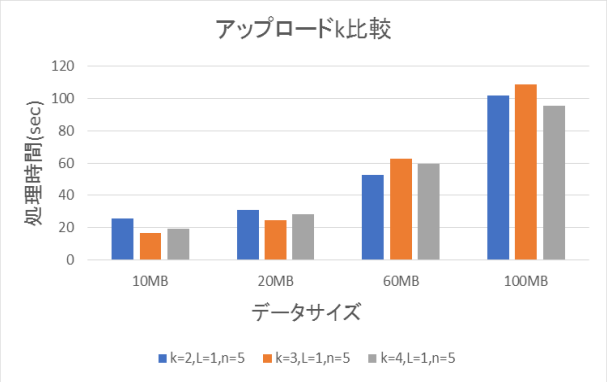


図.13 パラメータ k を変化させた時の提案手法のアップロード時間

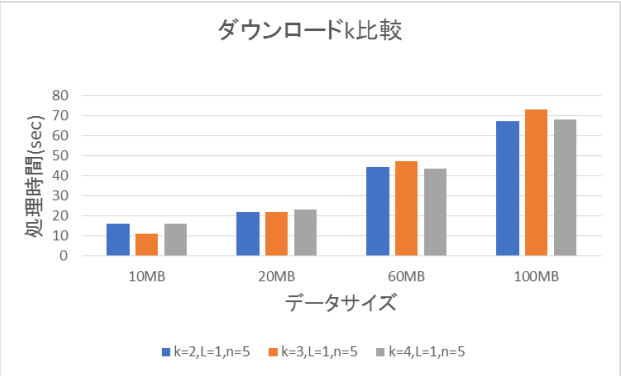


図.14 パラメータ k を変化させた時の提案手法のダウンロード時間

復号するための閾値であるパラメータ k を変化させた結果,ファイルのアップロードでは,閾値に関係なく分散した数だけファイルを送信する必要があるため変化が見られないと予想され,実測値でもその結果が見られている.提案手法は基本的にダウンロードの処理をマルチスレッドで処理を行っているが,シングルタスクになっている部分もあるがため,閾値が増えるにしたがって処理時間が長くなると予想されるが,実測値では処理時間にあまり変化は見られない.

次にパラメータ k,L,n のうち k を 4,n を 5 に固定して L を変化させた場合に提案手法の処理時間がどのように変化するかをファイル容量別に評価した.その結果を図 15,16 に示す.

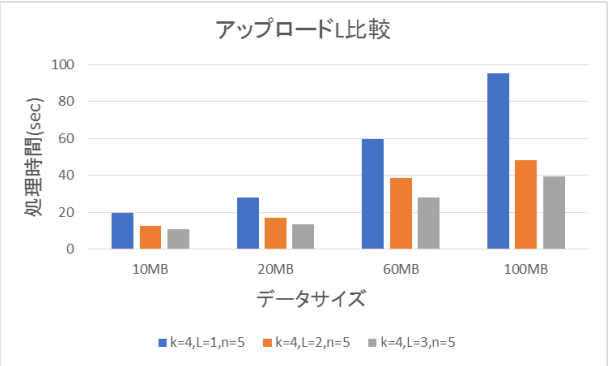


図.15 パラメータ L を変化させた時の提案手法のアップロード時間

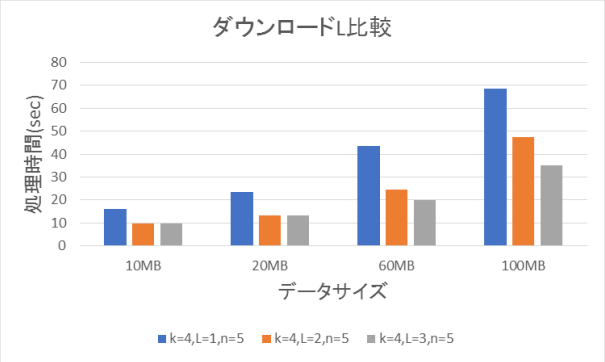


図.16 パラメータ L を変化させた時の提案手法のダウンロード時間

ファイル容量を減らすパラメータである L が増えるほどアップロード,ダウンロードの処理時間が減少していることがわかる.これはファイル容量の小さいものほど早くアップロード,アップロードができるため実装面でもその結果が見られている.

パラメータ k,L,n のうち k を 2,L を 1 に固定して n を変化させた場合に提案手法の処理時間がどのように変化するかをファイル容量別に評価した.その結果を図 17, 18 に示す.

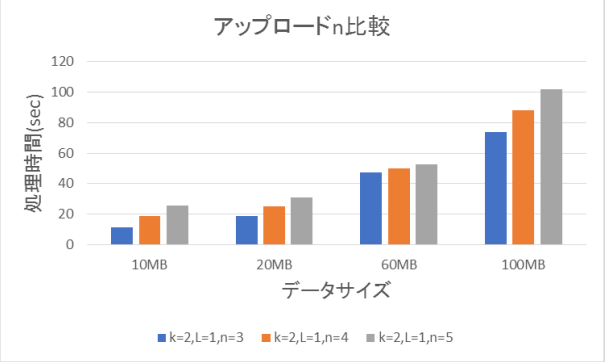


図.17 パラメータ n を変化させた時の提案手法のアップロード時間

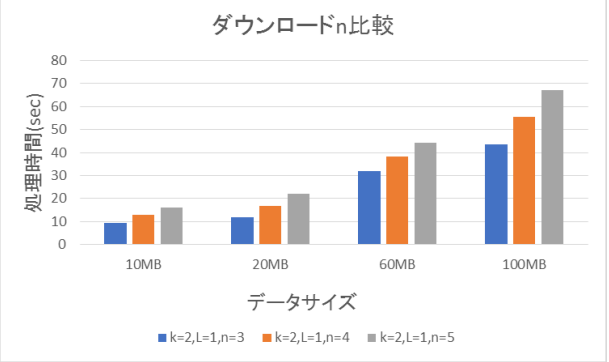


図.18 パラメータ n を変化させた時の提案手法のダウンロード時間

分散数を表す n が大きくなるほどアップロード,ダウンロードの処理時間は増えていることがわかる.提案手法は一部シングルタスクになっているため,アップロード時は分散数が多くなれば処理時間が増えることが予想され,実測値でもその結果が見られる.ダウンロードは閾値のファイルをダウンロードすればいいため本来は分散数によって処理時間に変化は見られないことが予想されるが,実装したシステムの想定では分散数が増えると処理時間も増えている.これはダウンロード時に一部シングルタスクになっていることが原因と考えられる.

7. 結論

本研究では,セキュアなクラウドストレージシステムの方式提案と実際のクラウドサービスを複数利用して実装したシステムの性能評価を行った.

高価なプライベートクラウドを導入することなしに,安価な複数のパブリッククラウドを利用し機密情報を保存するために,秘密分散法によりその情報を符号化する前に,その情報を共通鍵にて暗号化してから符号化する手法を提案し,高い安全性が得られることを確認した.秘密分散,暗号化,メッセージダイジェストなどを利用することで高い可用性と高い機密性を実現し,システム全体が一連の動作することを確認できた.これにより,セキュアな複数のパブリッククラウド利用を実現できた.

今後の課題として,本研究では動的に最適クラウドを選択していたが,選択するアルゴリズムの性能が低くクラウド選択が精密に行われなかった.そのため,アルゴリズムの性能向上することを検討する.また,アップロード,ダウンロード共に一部がシングルタスクになっているため,システム全体のマルチスレッド化による処理時間の高速化が課題となる.

参考文献

1) 角川歴彦, クラウド時代と＜クール革命＞, 角川書店(角川 one テーマ 21), March 2010.
2) 城田真琴, クラウドの衝撃, 東洋経済新報社, February 2009.
3) 丸山不二夫, “クラウドの成立過程とその技術的特徴について,” 情報処理, 2009.
4) A. Shamir, “How to Share a Secret,” Communications of the ACM, Vol.22, No.11, 1979.
5) G.R.Blakley, “Safeguarding cryptographic keys,” Proc. of the National Computer Confer-, 1979.
6) 山本博資, “(k, L, n)しきい値秘密分散システム,” 電子通信学会論文, Vol.168-A, No.9, 1985.
7) 尾形わかは, 黒沢馨, “秘密分散共有法とその応用,” 電子情報通信学会誌 Vol.82, December, 1999.