7ZA-04

Pub/Sub プラットフォームにおける委託型秘密分散法の実装

佐藤 友哉 † 大東 俊博 ‡ 近堂 徹 § 渡邉 英伸 ¶ 稲村 勝樹 ‖
東海大学 † 東海大学 ‡ 広島大学 § 広島大学 ¶ 広島市立大学 ‖

1 はじめに

災害時のデータ紛失等への対策として地理的に異なる拠点への分散バックアップが重要となっている．異なる地域のストレージはクラウドストレージを利用することで比較的容易に手配できるが，組織外のサーバを利用するため安全性には注意が必要である．分散バックアップに適した暗号技術として，情報理論的安全性と呼ばれる高度な安全性を有し，一部のデータが失われたとしても元データを復元可能な秘密分散法が知られている．2013 年に吉田らは通信帯域が狭いモバイル端末のような環境に適した委託型の秘密分散法を提案している [1]．この方式は利用者端末から送信された暗号文を分散処理する Frontend Server と暗号化分散情報から暗号化の効果を解除して Storage に保存する Backend Server から構成されている．なお，吉田らの方式におけるデータ転送は一般的な暗号化通信を想定しており，評価実験では HTTPS により実装されていた．

近年の IoT の普及により，不安定なネットワークを介して多数のセンサーデータが収集されるケースが生じている [2]．そこで，本研究ではこのような不安定なネットワークにおけるセンサーデータを安全に分散バックアップするために，Pub/Sub プラットフォーム上で吉田らの方式を実装する．提案システムでは，IoT デバイス・Frontend Server 間の暗号化データの受け渡しを Pub/Sub により実現することで，通信が不安定な環境でもセンサーデータを安定的に秘密分散処理に受け渡すことを可能にする．さらに，Backend Server での分散データの転送も Pub/Sub を利用することで並列処理を効果的に実行できるようにする．本稿では多様なメッセージングシステムに対して共通的なインタフェースを提供するソフトウェアライブラリ SINETStream[*1]を活用し，Pub/Sub プラットフォームとして Apache Kafka を用いた具体的な提案方式の実装を示し，その処理速度および通信速度を計測する．

2 吉田らの委託型秘密分散法

吉田らの方式 [1] では，Client はストリーム暗号でデータを暗号化をし，その暗号化データを Frontend Server (以下 FS と記す) で秘密分散法で分散処理する．

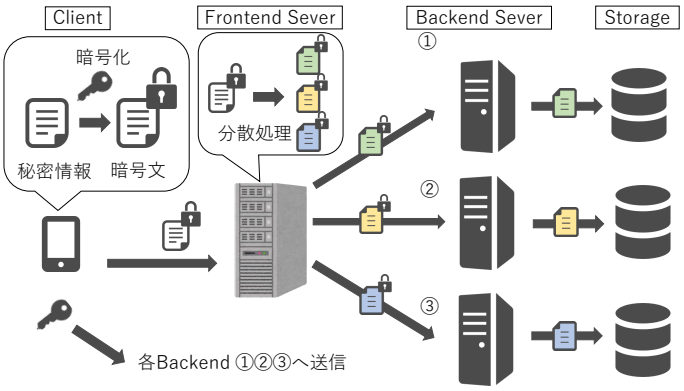

図 1 吉田らの方式の概要

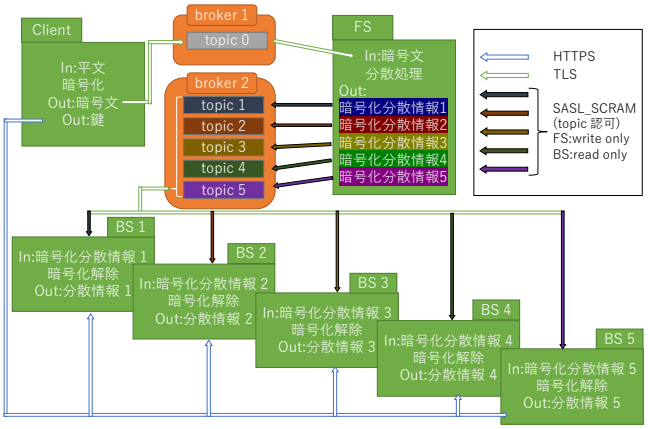

図 2 提案システムの構成

通常，秘密分散法のデータ量は分散数を n とした場合に暗号化データの n 倍のサイズになるため，吉田らの方式はモバイル端末からの通信量を $1/n$ に削減できている．このまま Storage に保存する場合，分散データを必要数 (k 個) 集めて復元すると暗号化データが得られるため，それを復号するための秘密鍵を管理するコストが発生してしまう．鍵管理コストの増大を回避するために，吉田らの方式では Backend Server (以下 BS と記す) においてストリーム暗号用の秘密鍵を用いた暗号化解除処理を実行することで，元データを秘密分散した場合と等価な分散データに変換してから Storage に保存する．暗号化解除処理は XOR 演算に基づく秘密分散法 [3] とストリーム暗号の暗号化の可換性を利用しているため，それらのタイプのアルゴリズムのみ利用可能である．吉田らの方式の処理手順の概要を図 1 に示す．Client は暗号化した後にその秘密鍵を BS に安全な通信路で送信し，

Implementation of Secure Outsourcing Scheme for Secret Sharing Scheme on Pub/Sub Platform
† Sato Tomoya, Tokai University
‡ Ohigashi Toshihiro, Tokai University
§ Kondo Tohru, Hiroshima University
¶ Watanabe Hidenobu, Hiroshima University
‖ Inamura Masaki, Hiroshima City University
*1 https://www.sinetstream.net/

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

表 1　提案システムにおける通信時間/処理時間 [sec]

	Client			Frontend Server		Backend Server
	BS へ鍵配布	暗号化	broker 1 へ暗号文を送信	分散処理	broker 2 へ暗号化分散情報を送信	暗号化解除
1KB	0.16440	0.00014	0.08863	0.00240	0.13145	0.00228
10KB	0.16392	0.00026	0.06751	0.00573	0.12813	0.00370
100KB	0.16325	0.00146	0.10473	0.01203	0.14640	0.01467
1MB	0.16472	0.01371	0.28763	0.11902	0.33357	0.10255
10MB	0.16686	0.13784	1.89842	1.19323	1.95021	0.96830

その後 FS に暗号文を送信して秘密分散を委託する．このとき FS と各 BS が結託しない，秘密分散法のパラメータ k 台以上の BS が結託しないという仮定のもと，元データは FS にはストリーム暗号による計算量的安全性，BS には秘密分散法の情報理論的安全性によって保護される．

3　Pub/Sub 通信モデル上での吉田らの方式の実現

Pub/Sub 通信モデルは非同期メッセージジングパラダイムの一種であり，出版社 (送信者) と購読者 (受信者) の間にあるメッセージブローカーを介して通信を行う．今回採用した Pub/Sub プラットフォームはトピックベースシステムである．

今回はストリーム暗号に AES-CTR モード，秘密分散法として $k = 2$，$n = 5$ のパラメータで XOR 演算に基づく秘密分散法 [3] を C 言語で実装した．通信は Client から各 BS への鍵配布は HTTPS，broker との Pub/Sub 通信は SINETStream を利用して Python で実装した．broker 1 では SSL/TLS 認証で通信を行い，broker 2 ではそれに加えて分散情報用に topic を設定し，FS には書き込み，各 BS には読み込み権限のみを付与している．

図 2 に Pub/Sub プラットフォームにおける吉田らの方式の実装図を示す．本稿の実装では Client，FS，各 BS, broker 2 をそれぞれ異なる VM 上で, broker 1 は実機上で docker コンテナとして構築している．提案システムでは，各機器の設置位置は Client, broker 1, FS は同一ネットワーク内，broker 2 は BS に近いネットワーク，Storage を BS と別に用意する場合は BS は Storage に近いネットワークに設置されていることを想定している．これは Client の通信時間をエッジコンピューティングの考え方で極力減らす目的と暗号化のみのデータは組織内のネットワークでのみ存在し，クラウドサーバでは秘密分散法で保護された高度に安全なデータにするという目的によるものである．

4　性能評価

提案システムの処理時間および通信時間の基本性能を確認するために評価実験を行った．実験では異なるデータサイズの平文に対して暗号化・分散処理・暗号化解除処理の処理時間および各 broker へ書き込む際の通信時間を計測した．Client，FS，broker 1 は東海大に設置しており，各 BS，broker 2 はさくらのクラウドに仮想サーバを立ち上げて構築している．

評価実験に用いた機器について述べる．Client と FS は Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz の実機上の Hyper-V でそれぞれ仮想マシン（コア数 1，メモリ 2GB）を作成して構築した．broker 1 は Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz，メモリ 32 GB の実機上に構築している．これらの実機は東海大学内のネットワークに設置している．次に broker 2 と各 BS は，さくらのクラウドにコア数 2（CPU: Intel(R) Xeon(R)CPU E5-2650 v3 @ 2.30GHz），メモリ 4 GB の仮想サーバを立ち上げて構築している．

表 1 に 10 回計測した処理時間と通信時間の平均値を示す．なお，分散処理，暗号化解除には broker からのデータの取得時間は含まれていない．実験の結果，10MB のデータを分散バックアップする場合，Client で broker 1 へ書き込むまでの処理時間・通信時間の合計は 2 秒程度であることが分かった．さらに，FS が暗号化データ取得後に分散情報を broker 2 へ書き込むまでの時間は 3 秒程度，BS が分散情報取得後に暗号化を解除するまでの時間も 1 秒程度となった．また，データ転送に Pub/Sub を利用した場合に通信時間が極端に大きくなっていないため，実用に耐える時間で委託型秘密分散を実現できたと考えている．

5　おわりに

本稿では IoT デバイスから取得するセンサーデータのセキュアな流通基盤として，委託型秘密分散法を Pub/Sub プラットフォームを組み合わせた方式を実装した．従来方式との比較や，広域かつモバイル環境における計測が今後の課題である．

謝辞

本研究の一部は JSPS 科研費 19K11971，20K11811，21K11846 および 2021 年国立情報学研究所公募型共同研究 (21S0603) の助成をうけて実施している．

参考文献

[1] 吉田耕太, 西村浩二, 大東俊博, 相原玲二,“ 秘密分散法を利用したクラウドストレージサービスにおけるモバイル機器を考慮した安全な処理委任方式” 情報処理学会論文誌, vol.55, No.3, pp.1117-1125, 2014 年 3 月.
[2] 近堂 徹，町澤 まろ，“脳生理情報のクラウド解析プラットフォーム実現に向けた通信手法の検討，” DICOMO 2021 論文集, pp. 237–242，2021 年.
[3] 保坂範和, 多田美奈子, 加藤岳久,“秘密分散法とその応用” 東芝レビュー, vol.62, No.7, pp.23-25, 2007 年.

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.