講演番号：58

セキュアーSNS を実現する分散データベース方式の検討

B－7　　Study of Distributed Database System for Realizing Secure SNS

剱持 遼太郎† 篠原 峻輝† 宮保 憲治†
Ryotaro KEMMOCHI† Shunnki Shinohara Noriharu MIYAHO† †
† 東京電機大学 情報環境学部 情報環境学科
† School of Information Environment, Tokyo Denki University

1. はじめに

現代のネットワーク社会において Facebook, Twitter などの SNS はコミュニケーションや情報収集の手段として定着しつつある．しかしながら，システムの脆弱性により，情報漏えいやアカウント乗っ取りなどの被害に遭遇する可能性も高いことが指摘されている．このため，サービス提供者側は，特にＩＤやパスワードを含めた個人情報の管理保全を容易に徹底化できるメカニズムを導入することが急務の課題となっている．

この状況に鑑み,本稿では重要電子データのバックアップに用いる HS-DRT（High Security-Disaster Recovery Technology）[1]を適用した新しいセキュアな SNS サービスの方式提案を行い，計測結果に基づいた性能評価を述べる．

2. 提案するセキュア SNS

提案するセキュア SNS のシステムの構成を図1に示す．

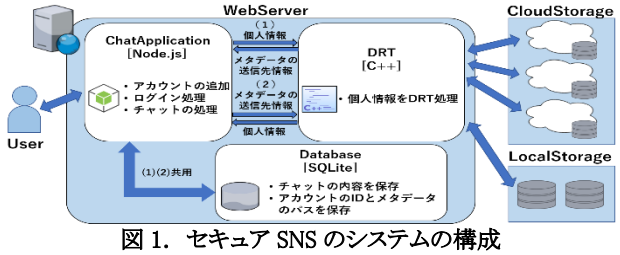

図 1. セキュア SNS のシステムの構成

提案方式ではデータベースに個人情報を，直接，格納することはせず，アカウントの ID・パスワードと紐付けされたメタデータの送信先情報のみを格納するメカニズムを採用することでセキュアな SNS サービスを実現できる.具体的には，ユーザがアカウントを登録する際に,入力された個人情報を,システム側では事前に秘密に設定したストリーム暗号と，一体化処理（情報の空間的攪拌）を組み合わせて暗号化後，複数のファイルに分割する（以後,断片ファイルと呼称）.また，元の個人情報に復元するために必要な鍵情報が記述されたファイル（以後,メタデータと呼称）も同時に作成する.これらの全てのファイルを閾値秘密分散方式に則り,クラウド（ローカル）ストレージに送信する.データの送信後,アプリケーション側にメタデータの送信先情報が返信されるので,アカウントの ID と紐付けてクラウドのデータベースに格納する.個人情報自体はクラウドに格納されないため,データベース内の情報が仮に盗み取られた場合でも個人情報の流出には繋がらない.クラウドストレージ内のデータが漏洩した場合でも,データそのものはランダムな文字列に暗号化されているため個人情報は漏洩したとしても影響がない.ユーザはログイン時に ID/パスワードを入力し,対応するメタデータの送信先情報を元に，予め設定された暗号処理プログラムが起動され，個人情報を復元できる.その後,復元された個人情報内のパスワードと入力されたパスワードとを比較し,一致した場合のみログイン処理を行うことで，安全性を担保できる.

3. 性能評価

3.1. 実験用チャットアプリケーション

提案方式の性能評価を行うため,前述の暗号処理機能を搭載した実験用チャットアプリケーションを作成した.当該アプリケーションは，C++, Node.js, SQLite を用いて実装した.

3.2. 性能評価結果

アプリケーション上で個人情報のファイルサイズを変化させ，以下に示す DRT 処理の実行時間を計測した.

(1) Node.js から C++に個人情報を渡してメタデータの送信先情報として返却されるまでの暗号処理時間
(2) 送信先情報を渡して個人情報が返却されるまでの復号処理時間

個人情報のファイルサイズは 100KB～100MB まで変化させ,HS-DRT 処理の適用時は,一体化処理 6 回,分割数 60,断片ファイルは(2,3),メタデータは高い安全性に配慮し,(4,7)閾値秘密分散処理を採用した.データの送信先はローカルディレクトリに置いた.図2に計測処理時間を示す.

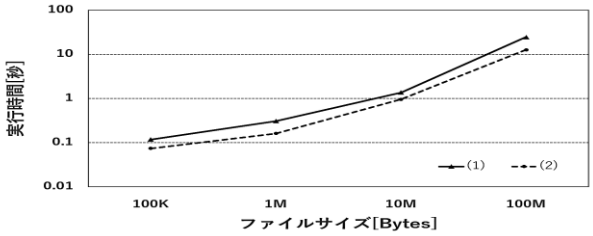

図 2. DRT 処理の実行時間

図 2 より,1MB 以下のデータ量では DRT 処理実行時間はどちらの処理も 0.5s 以下を実現でき,個人情報を扱う場合としては十分な応答性能が得られることが判明した.

4. まとめ

HS-DRT 技術を活用することで,ユーザの個人情報を安全に管理する SNS サービスの方式を提案した.今後は同時接続可能なユーザ数を考慮すると共に,個人情報だけでなく,画像やチャットの内容も高速暗号化処理を実現できるシステム構築を行う予定である.

参考文献

[1] N.Miyaho, et.al., "Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications" IARIA Journals, vol.3, no.1, pp. 266-278, 2010.