IPA

2023 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

竹迫 良範（株式会社リクルート データプロダクトユニット ユニット長）

2. クリエータ氏名

福山 将英（慶應義塾大学 環境情報学部 環境情報学科）

3. 委託金支払額

2,736,000 円

4. テーマ名

TEE を用いたセキュアかつ高性能なデータベースシステムの開発

5. 関連 Web サイト

ソースコード：https://github.com/Noxy3301/CASSA

6. テーマ概要

クラウド事業者が信頼できない状況下でも、機密性と性能を両立するデータ基盤 CASSA（Cloud-Adapted Secure Silo Architecture）を開発した。このシステムは、Intel SGX の 1 つである Scalable-SGX を用いて Enclave のメモリ制限を緩和し大容量を扱えるようになった。また、トランザクション処理プロトコルに Silo、索引に Masstree を採用し、データの処理性能と機密性を向上させた。

7. 採択理由

本プロジェクトは、Intel SGX v2 を用いて、KVS インタフェースを持つセキュアで高性能なデータベースシステムを自作するという野心的な提案である。従来のインメモリデータベースで使われていた Silo というトランザクション処理技法を TEE 上の隔離実行環境の中で動かすことで、セキュリティと高性能を両立させることを狙っている。

似たようなコンセプトでオープンソースとして公開されている従来の実装としては ShieldStore があるが、古い Intel SGX v1 で開発されており、128MB のメモリサイズ上限が存在するため、インメモリデータベースを実装するには不

適当なアーキテクチャである。

今回開発する実装は Intel SGX v2 のため 512GB まで対応が可能になる見込みである。ログは暗号化した状態で WAL を行い、並列ログ書き込みできるのであれば他システムと比べても優位性があると考えられる。

セキュアなトランザクション処理技法については、論文上でいくつかの提案はあるが、ソースが公開されていないものも多い。本プロジェクトによって新しく Intel SGX v2 で実装した TEE 上の Silo データベースシステムがオープンソースとして公開され、セキュアで高性能なデータベースシステムの実用性が向上することを期待し、本提案を採択した。

8. 開発目標

クラウド事業者は自身の計算資源の管理者権限を有しており、理論上メモリ上のデータを読み取ることができるため、クラウドサービス提供者を無条件に信頼できない場合においてデータの機密性保持が課題となっている。Intel SGX によって提供される隔離実行環境 Enclave を活用し、クラウド事業者が信頼できない条件下でもクラウド上の機密性を保証できるシステムを開発することが目標である。

9. 進捗概要

本プロジェクトで開発した CASSA のアーキテクチャを図 1 に示す。

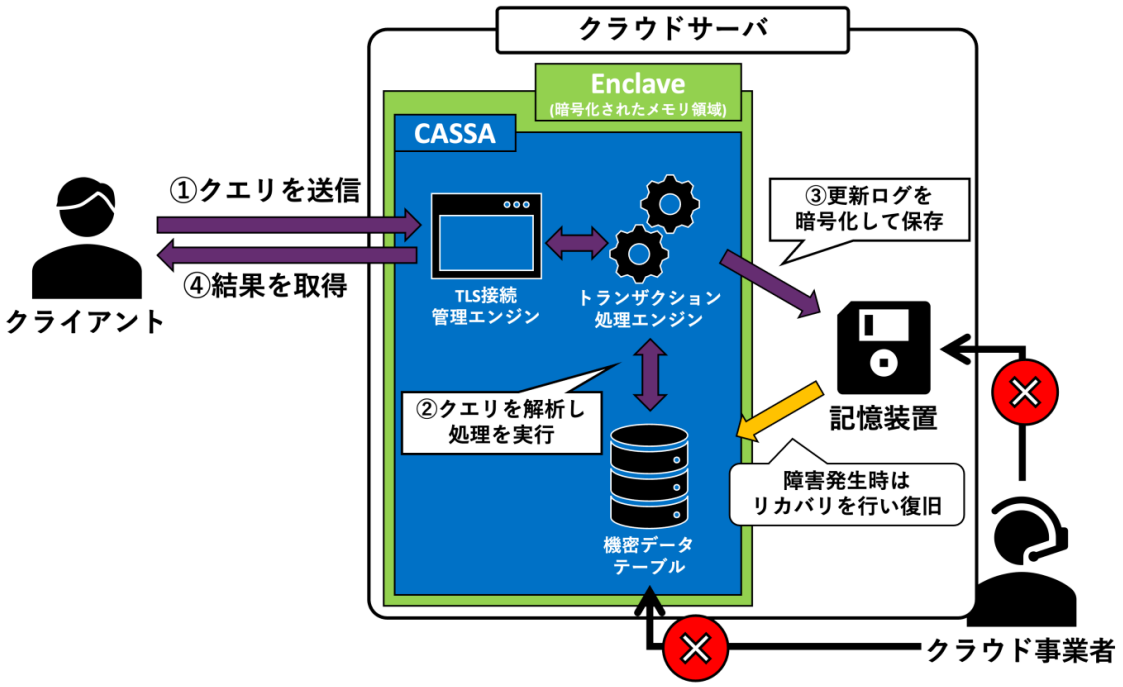

図 1：開発した CASSA のアーキテクチャ

① クライアントは、TLS セッションを通じて、CASSA にクエリを送信する。
② CASSA はクエリを解析し、Silo と Masstree を用いてデータの検索、更新を行う。
③ クエリによるデータベースの改変内容は、必要に応じてログを作成し、暗号化してストレージに書き込みを行う。
④ ログ書き込み後、クライアントに結果を返送する。

このシステムは、Intel SGX の 1 つである Scalable-SGX を用いて隔離実行環境 Enclave のメモリ制限を緩和し、トランザクション処理プロトコルには Silo を、索引には Masstree を採用した。これにより、データの処理性能と機密性を向上させた。さらに、Intel SGX の機能の一つである Remote Attestation を活用し、意図した通信相手が Enclave 内で正しいプログラムを実行していることを保証しつつ、TLS セッションを確立することで、通信相手と通信経路の機密性と真正性を保証した。システムの耐故障性付与のためのログに関しても、暗号化して保存することで、クラウド事業者による不正な観測や操作を防ぐようにした。信頼できないストレージ上のログデータは欠損するリスクがあり、完全性保証のため、CASSA はログ改ざん検知プロトコルを導入した。これにより、ログの欠損や改ざんを検知可能にし、システムの完全性と真正性を保証することができた。

10. プロジェクト評価

Intel SGX が提供する隔離実行環境内の Enclave で動作する、性能と機密性を両立するデータベースシステムを構築できた。Intel SGX の複雑性を抽象化し、システムに開発者が Intel SGX の制約下で任意の処理を実装できる仕組みを別途用意することができた。当初の設計では、各クライアントがサーバ上で独自のデータベースシステムを運用する想定だったが、クライアントとサーバのアプリケーションを個別に実装し、ECDSA Attestation による真正性保証付き TLS セッションを確立することで、1 対多のシステムを構築可能にした。これによって、データの保存だけでなく、処理を含む幅広い応用が可能になった。開発したシステムのベンチマークを測定したところ、YCSB-A ワークロードで 60 トランザクション並列処理時、最大 228 万 tps の処理能力を達成した。Intel SGX 特有の煩雑さを抽象化しつつ、機密性と性能を両立できた。

11. 今後の課題

現行の Silo の実装では各操作命令の成否を早期に評価して失敗時に即座にトランザクションを中断する簡易的な方式となっており、性能向上の妨げになっている。このような Silo の簡易的な比較ロジックを削除し、楽観的並行性制御法の性能向上を図る必要がある。また Masstree の実装では、マルチバージョン

並行制御法を採用することで更新処理の性能を向上させる余地が残っている。TLS 接続管理エンジンにおいて、Intel SGX の制約によるポーリング方式は CPU リソースを大量に消費するため、イベント駆動などの効率的な管理方法を検討する必要がある。Intel SGX の Enclave 内の並列動的メモリ割り当ての遅さが性能評価に大きな影響を及ぼすため、性能劣化の原因追及と対策が必要である。