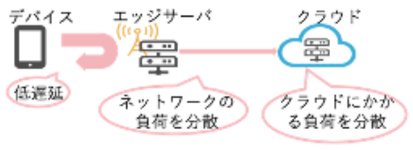
小口研究室　研究紹介　(2022年度)
(お茶の水女子大学理学部情報科学科)

リッチクライアント–エッジサーバ間におけるプライバシ保護に優れた分散機械学習
（研究担当:高野　紗輝）

研究背景

◆ スマートフォンやIoTデバイスの普及
◆ 機械学習の活用機会が増加 → エッジデバイスで収集した大量のデータに対してプライバシを保護しながら複雑な処理を行うことが求められる

◆ デバイスに近いネットワークエッジにエッジサーバを配置して処理を行うエッジコンピューティングが注目されている
◆ しかし、性能の低いエッジデバイス側はあくまでデータを収集し、そのデータをエッジサーバに転送するという役割



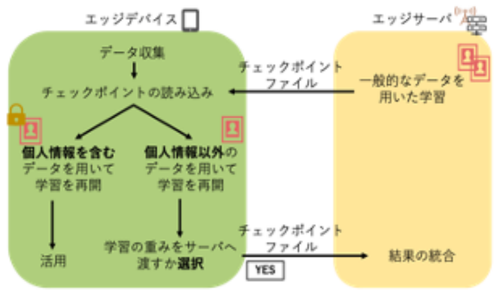
研究目的

◆ 研究課題
1. プライバシの保護
2. エッジサーバに渡すことができないエッジデバイス上のデータを含めた機械学習

◆ 研究目的
複雑な処理も行うことのできるリッチデバイスの登場
⇩
リッチデバイスに適した分散機械学習モデルの構築

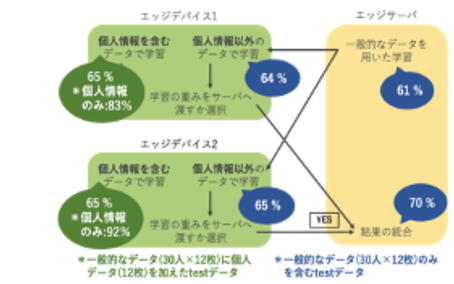
提案モデル

◆ エッジコンピューティングにおいて従来エッジサーバ上で行っていたタスクの一部をエッジデバイスにオフロードする



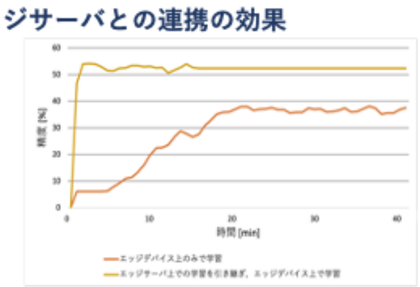
- エッジサーバ上での学習をエッジデバイスで引き継ぐ
- エッジサーバへフィードバックするかユーザが選択可能

実験



✓ 一般人物のデータのみではなく個人データに関しても高い精度で判別が可能
✓ フィードバックによって初め61%だった精度が70%まで向上

エッジサーバとの連携の効果



✓ エッジデバイスのみでの学習にはかなりの時間がかかる
✓ エッジデバイスで収集された一般人物のデータの枚数はエッジサーバに比べ少ないため，精度が低い結果となる
→ エッジサーバの助けを借りることが有効

エッジサーバと**連携**しつつ，エッジデバイス上でも学習を行うことによって**一般人物・個人情報共に短時間で知見を得ることが可能**

本提案モデルはエッジサーバに結果を渡さない選択が可能
→ **プライバシ保護に優れている**

ユーザの許可を得たエッジデバイス上での学習結果をエッジサーバへ**フィードバック**することで**より良い結果が取得可能**

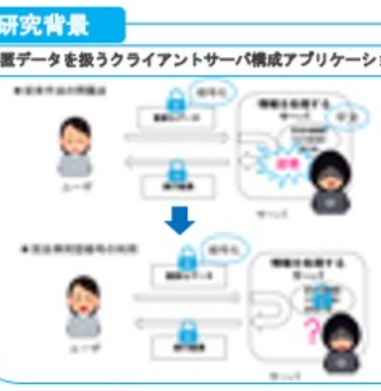
今後の課題

◆ データを変化させた実験
◆ フィードバックを行う情報を制限することによる細かい制御の検討

完全準同型暗号アプリケーション実行時の課題に対する 高性能SSD適用手法の評価
（研究担当:廣江　彩乃）

研究背景

秘匿データを扱うクライアントサーバ構成アプリケーション



完全準同型暗号

- 暗号文同士での加算・乗算が可能な暗号化手法
- 盗聴されても復号が難しいため、セキュリティ対策として大変有用
- 実行時間の課題により実用化に向けた研究開発が進む

課題

- 完全準同型暗号利用による長い実行時間
- 大量のメインメモリ需要
- コンピュータリソースにかかる莫大な費用

研究開発が進む高性能記憶装置

不揮発性で安価であるHDDなどの性能と、レイテンシが短いメインメモリの性能の両方を合わせ持つ記憶装置の研究が進む
(ストレージクラスメモリとも呼ばれる)

研究目的

✓秘匿データを扱う機会の急増に伴い、高まる完全準同型暗号暗号化アプリケーションへの需要
✓一方で、実行時間や費用の面からコンピュータリソースに関する課題がある
✓本研究では、**クラウドを想定した費用対効果の課題に対して高性能記憶装置の活用**を検討

実験手法

✓ Dockerコンテナを使用し、メインメモリが不足する状況を再現
✓ 完全準同型暗号を用いたアプリケーションのパラメータであるクエリ長を4, 5, 6として段階的に処理内容を増大させ、実行時間を計測

表1：用いた記憶装置

種別	不揮発メモリ	SSD			
製品名	Intel Optane 200 Series	Intel Optane 905P	EXCERIA PLUS	SAMSUNG SSD 980 PRO	INTEL SSDPEKKW010T8
搭載メモリ	3D XPoint (低レイテンシ)		3D NANDフラッシュ		
接続方式	DDR-T (メモリバス)		NVMe		SATA

表2：各条件におけるメモリ割当

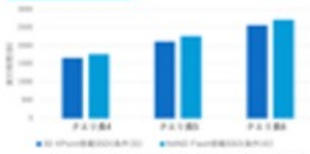
	条件1	条件2	条件3	条件4	条件5	条件6
使用可能メモリ	十分	1GB				
Swap領域	Swap発生なし	不揮発メモリ	Intel Optane SSD (3DXPoint)	Samsung SSD	Kioxia SSD	Intel SSD (NAND Flash)

実験結果

表3：実行時間

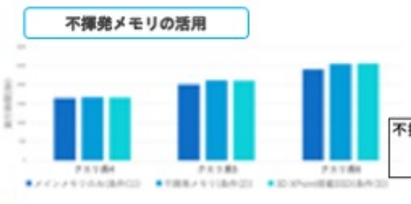
		クエリ長4	クエリ長5	クエリ長6
条件1	メモリ制限なし	27分34秒	33分37秒	40分16秒
条件2	不揮発メモリ	27分53秒	35分18秒	42分41秒
条件3	Intel Optane 905P	27分46秒	35分16秒	42分47秒
条件4	Samsung 980 PRO	29分33秒	37分46秒	45分18秒
条件5	KIOXIA-EXCERIA PLUS	32分16秒	41分31秒	50分31秒
条件6	Intel SATA	36分53秒	47分23秒	57分15秒

搭載メモリ



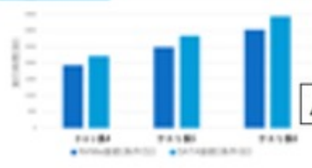
低レイテンシな3D Xpointメモリは実行時間短縮に有効

不揮発メモリの活用



不揮発メモリの効果は本実験では得られなかった

接続方式



NVMe接続とSATA接続では4-6分ほど顕著な差が出た

まとめ

1. メモリバスに挿して用いる不揮発メモリと，PCIスロットに挿して用いるSSD桁違いの差が出ることが予想されたが、今回のアプリケーション実行では差が出なかった
2. 低レイテンシな3D XPointメモリを搭載したSSDは実行時間短縮に有用
3. PCIスロットとSATA接続では実行時間に顕著な差が出た

無線および有線環境を考慮した輻輳制御ミドルウェアにおける輻輳ウィンドウ制御の一検討
（研究担当:松野　瑛南）

研究背景

- スマートフォンの市場の拡大
  - 高性能
  - 持ち運びに便利

端末の高性能化
通信性能に差がある端末での同時通信

ボトルネック
有線/無線環境で発生する輻輳を制御

大容量データ通信
(ex: ライブ配信の視聴)
→ 通信障害 → **輻輳**発生
トラフィック量増加

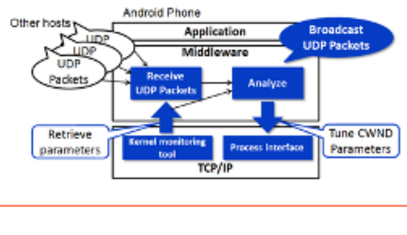
輻輳制御ミドルウェアの改良
合計通信速度 / 公平性 の向上を目指す

先行研究

輻輳制御ミドルウェア

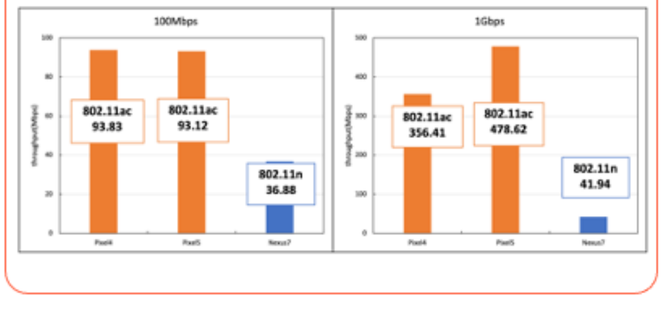
APに接続した端末間を連携することで
お互いの接続状況を把握しCWND を設定

→ **合計通信速度 / 公平性 向上**



基礎実験

- 端末の通信性能を測定
  通信速度の大きな差の原因: Android OS / 無線規格の差異



提案指標

- 通信性能に**重み**をつけた公平性の指標
- 取得した通信速度を最大通信速度の値で割った値を代入

$$F_j(X_n) = \frac{\left(\sum_{i=1}^{n} x_i\right)^2}{n\sum_{i=1}^{n} x_i^2}$$

既存指標

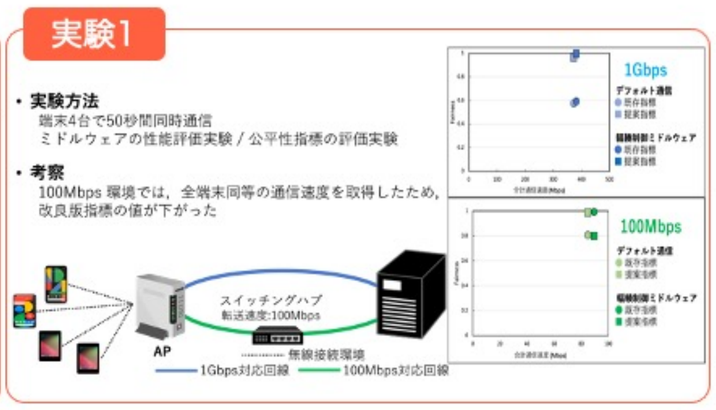
$$x_i \rightarrow \frac{x_i}{Max_i}$$

$$F_j(X_n) = \frac{\left(\sum_{i=1}^{n} \frac{x_i}{Max_i}\right)^2}{n\sum_{i=1}^{n} \frac{x_i}{Max_i}^2}$$

提案指標

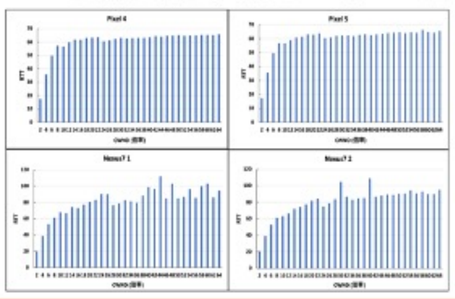
実験1

- **実験方法**
  端末4台で50秒間同時通信
  ミドルウェアの性能評価実験 / 公平性指標の評価実験
- **考察**
  100Mbps 環境では，全端末同等の通信速度を取得したため，改良版指標の値が下がった



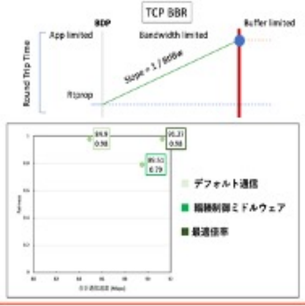
実験2

- TCP BBR を参考に RTT とCWND の関係性を調査
- CWND基準値を設定し，変化させた時のRTTを測定



- パケットがキューから溢れない最適倍率を探索
- 求めた最適倍率を端末に導入し，同時通信を行う
  → 合計通信速度，公平性の向上を確認

自動探索プログラム 最適倍率	
Pixel4	8倍
Pixel5	8倍
Nexus7-1	10倍
Nexus7-2	14倍



https://www.is.ocha.ac.jp/~oguchi_lab/　　oguchi@is.ocha.ac.jp