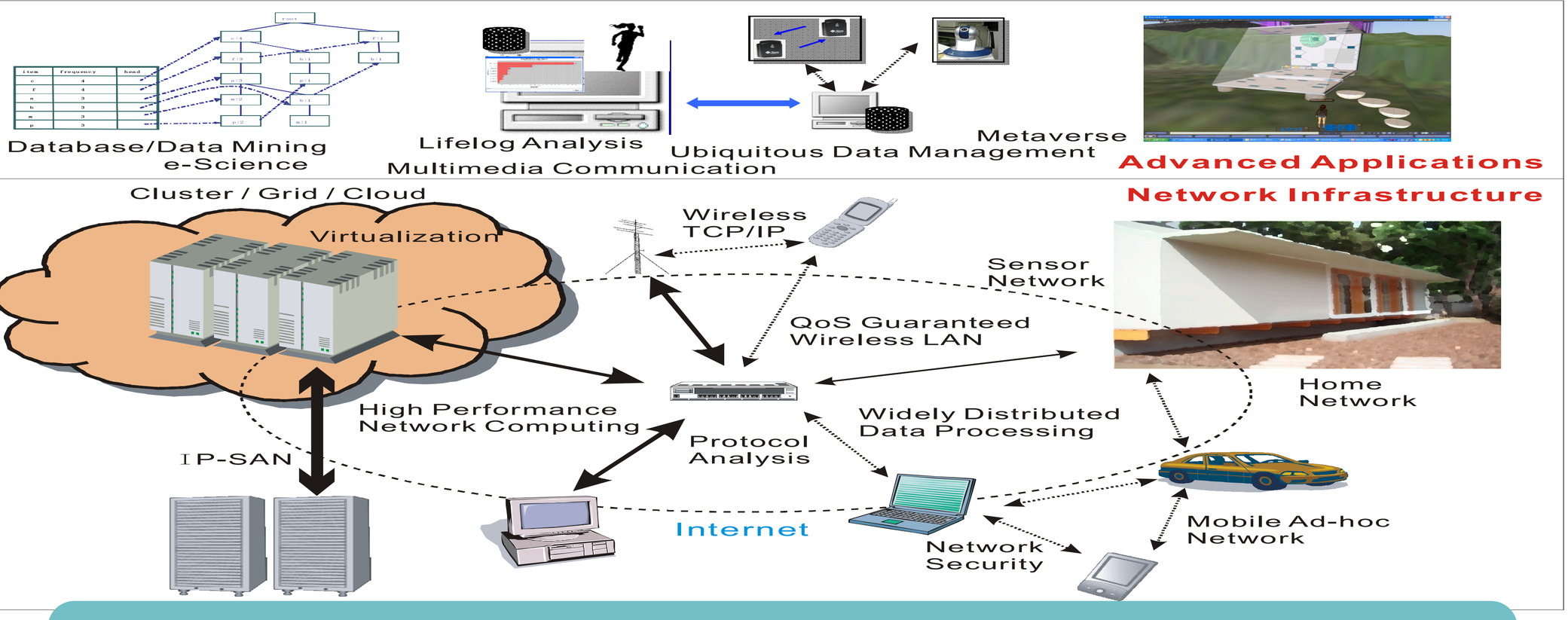
小口研究室　研究紹介　(2022年度)
(お茶の水女子大学理学部情報科学科)

次世代ネットワークコンピューティング基盤と先進的アプリケーション



◆研究テーマ：ネットワークコンピューティング・ミドルウェア

- ●多種多様な通信・計算機器が複雑に結びついて情報化社会のシステムを形成
- ●次世代ネットワークコンピューティング基盤に焦点を当て、先進的アプリケーションそれを支えるミドルウェアを研究

Querying Multi-Attribute Records with Inner Product Encryption
（研究担当:松本　茉倫）

Overview

- **Leakage of a scheme based on deterministic encryption (DET)**
  - The leading cryptography-based DBMS, such as CryptDB, MONOMI, explore DET.
  - DET is suffered from leakage of data frequency and search patterns.
- **The disadvantage of fully homomorphic encryption (FHE)**
  - FHE can prevent leakages, but homomorphic operations are much slower than plaintext operations.
  - The size of FHE ciphertext is storage-intensive.
- **New querying scheme *IPEQ* with function-hiding inner product encryption (FHIPE)**
  - The DB server only view the result of a query by computing **⟨x, y⟩** with the record as vector **y** and the query condition as vector **x** as shown in Figure 1.

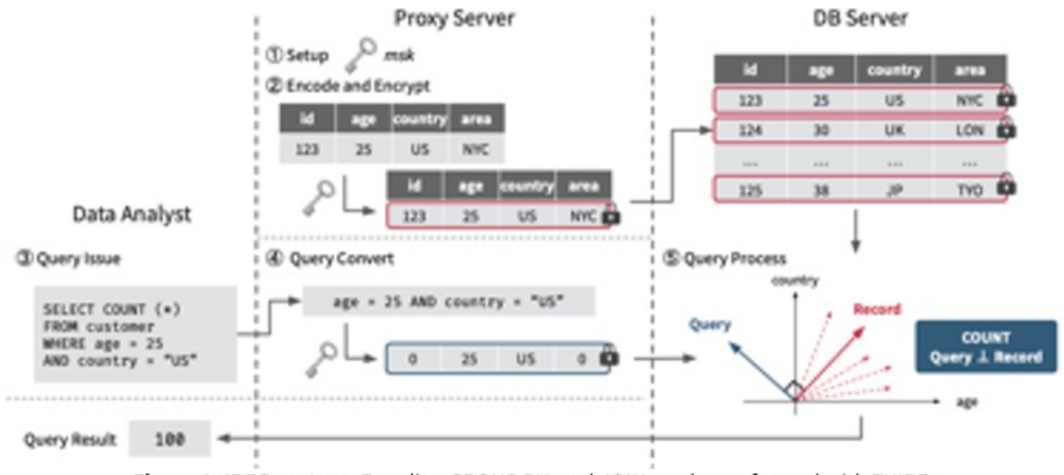


Figure 1: IPEQ system. Equality, GROUP BY, and JOIN can be performed with FHIPE.

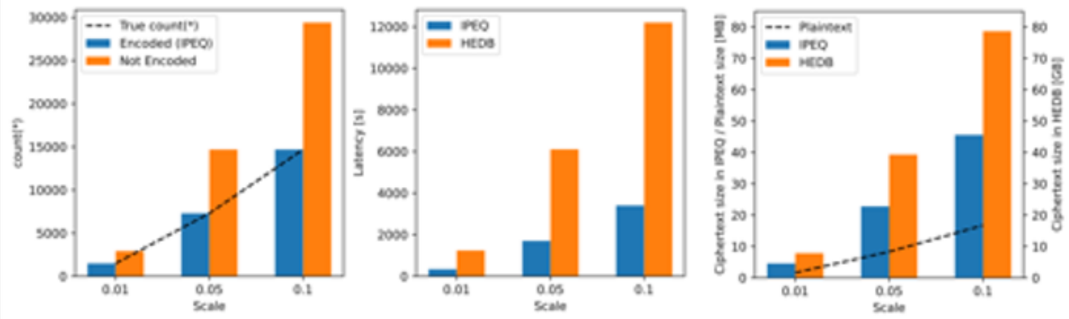
Main challenge

1. **The query does not always return the correct value for the multi-attribute records.**
   e.g.) SELECT COUNT(*) FROM T WHERE age=25 AND country_cd =2
   Query **x** = (-25-2, 1, 1)
   Record **y** = (1, age, country_cd)
   } age=25 AND country_cd=2 ⇒ **⟨x,y⟩**=0 means the condition matches.
   but, (age=23 AND country_cd=4), (age=26 AND country_cd=1) ⇒ **⟨x,y⟩**=0
2. **The JOIN key must represent a wide range of values.**
   → Simply expanding the plaintext space results in high latency.

We must encode records for efficient and accurate queries !

Evaluation

- We use orders dataset from TPC-H benchmark. Orders with a scale factor of 0.01 contains 15,000 rows.



(a) Multi-attribute query accuracy **(b) IPEQ vs. HEDB (Latency)** **(c) IPEQ vs. HEDB (DB size)**

Figure 2: (a) Our encoding of the record and query conditions can preserve query accuracy. (b)(c) IPEQ outperforms homomorphically encrypted DB (HEDB) in terms of query execution latency and DB size.

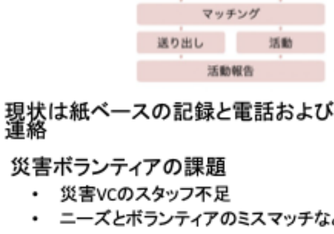
災害時ボランティア支援アプリケーションのCordovaを用いた実装
（研究担当:関口　穂波）

研究背景

- 近年、地震や台風などの大規模自然災害が多く発生している
- 被災地では外部からのボランティア支援の受け入れ態勢を整える必要がある
  →地域の社会福祉協議会とNPOを中心に災害ボランティアセンター（VC）を設置
- 現地に来たボランティアと被災者から聞いたニーズとを対応させる（マッチング）
- 現状ではマッチングは全て手作業で行われており、時間がかかっている

研究課題

- 災害ボランティアのマッチングの流れ



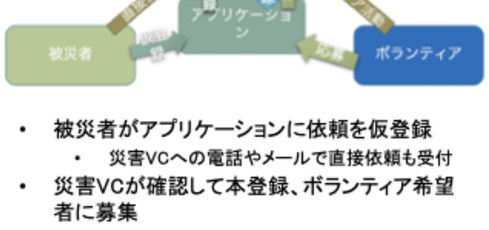
- 現状は紙ベースの記録と電話および対面による連絡

→ 災害ボランティアの課題
  - 災害VCのスタッフ不足
  - ニーズとボランティアのミスマッチなど

- 電子化・オンライン化する事により、広範囲で迅速な情報共有が実現可能
- 現状の流れを置き換えるボランティア支援アプリケーションが必要

アプリケーションの設計

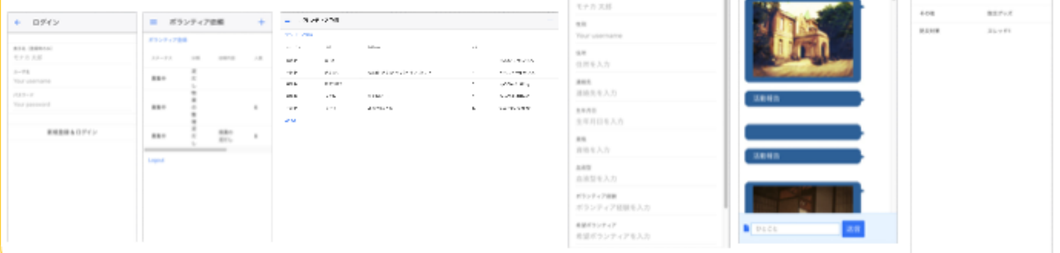
- 提案アプリケーションの流れ



- 被災者がアプリケーションに依頼を仮登録
  - 災害VCへの電話やメールで直接依頼も受付
- 災害VCが確認して本登録、ボランティア希望者に募集
- ボランティア希望者はボランティア依頼を確認して応募
- 依頼の条件により災害VCがマッチング
  - 将来的にはマッチング自動化も検討

アプリケーションの実装

- Cordova開発環境でWindows, iOS, Androidプラットフォーム向けのアプリケーションをWeb開発技術のみを用いて開発
- ログイン画面
  - 一般ユーザと管理者のログイン
- ボランティア依頼一覧画面と災害VC側での確認画面
  - 災害VC（管理者側）…全て確認可能
  - ボランティア依頼者…自分の依頼確認可能
  - ボランティア希望者…災害VCで公開された情報確認
- ボランティア情報登録画面
  - 災害VCで用紙に記入している情報をDB化
- チャット画面
  - ボランティア活動中のグループ内の情報交換と活動後の災害VCへの報告資料作成
- 掲示板画面
  - 平時に利用可能な情報共有機能も実装



まとめと今後の課題

- 大規模災害時に設営される災害VCと被災者およびボランティアの支援アプリケーションを実装
- 災害VCにおける人手不足解消と労力削減・情報共有を実現
- 電子化・オンライン化によって、より多くのボランティアの参加を促進
- 災害VCを設営する社会福祉協議会、被災者、ボランティアに使用してもらい評価とフィードバックを得る

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