論 文 内 容 の 要 旨

博士論文題目　Privacy-Aware Platform for Smart Home Sensor Data
（スマートホームセンサデータのプライバシアウェアプラットフォーム）

氏　　名　　Sopicha Stirapongsasuti

（論文内容の要旨）

The development of sensors and smart appliances can offer many smart home services, e.g., smart appliance control, anomaly detection, life logging, and elderly monitoring. However, data from these devices may contain privacy-sensitive information, which could be misused by attackers using machine learning. Previous studies applying privacy mechanisms often decrease service utility such as activity recognition accuracy. To protect privacy-sensitive data in smart home systems using untrusted cloud infrastructure, we propose a system with four modules: 1) smart sensors/appliances, 2) home gateways transferring data to a cloud or edge server, 3) edge servers modifying data to protect privacy, and 4) a cloud server storing/analyzing data to generate services. We assume a threat model where an adversary can access data in the untrusted cloud server during certain time slots, while residents' data upload demands vary over time. We propose two privacy mechanisms. The first is controlling the upload of smart home data to preserve privacy while maintaining service benefits. This involves choices of upload data type (raw or recognized activity label), upload frequency, timeslot-based risk and benefit assessment, and optimal choices in each time slot considering trade-offs between risk and benefit. We formulate a combinatorial optimization problem to determine the data type and upload frequency in each time slot, considering edge server resource constraints and user preferences. A heuristic algorithm provides semi-optimal solutions. Simulations using the CASAS dataset showed higher benefits with lower risk compared to conventional methods, emphasizing the importance of supporting users' decisions on data uploads to preserve privacy. The second approach uses Rényi differential privacy (RDP) to preserve privacy but we found that using only RDP decreases data utility. Thus, we propose feature merging anonymization (FMA) to preserve privacy while maintaining data utility by merging feature data frames of similar activities from different homes. The expected trade-off is defined so data utility should exceed privacy preservation. Evaluating the techniques using the HIS and Toyota datasets, FMA lowered person identification accuracy to 73.85% and 41.18% (from 100%) while maintaining activity recognition accuracy at 94.62% and 87.3% (compared to 98.58% and 89.28%). Further experiments explored implementing FMA in a local server, showing the local server can still meet the expected trade-off at some merging ratios.

氏　名	Sopicha Stirapongsasuti

（論文審査結果の要旨）

センサやスマート家電の普及により、スマートホームサービスが可能になったが、プライバシーの高い情報が含まれているため、悪意ある攻撃者による再識別（行動を行っている人の特定）のリスクがある。これに対し、データにプライバシー保護処理を適用する研究が行われているが、サービスの有用性が低下する問題がある。

本論文では、スマートホームデータに対する 2 つのプライバシ保護機構を提案し評価した。

本研究の学術的貢献は以下のとおりである。

1. スマートホームデータのアップロードを制御する方法を提案した。プライバシを保護しながらサービスの有用性を保持するために、エッジサーバリソースとユーザの予算、行動の k 匿名性、ユーザの好みを考慮した時間帯ごとのデータタイプとアップロード頻度の選択を目的変数とする組み合わせ最適化問題を定式化し、準最適解を導くヒューリスティックアルゴリズムを開発した。また、スマートホームのオープンデータセットを使用したシミュレーションを通じて、提案方法が従来の方法よりも低リスクで高い効用を達成し、予算が多いほど効用を大きくできることを示した。
2. プライバシを保護しながらデータの有用性を維持するために、行動を撮影した画像データから算出される HOG 特徴量に差分プライバシを適用し、他の家庭の同じ行動の特徴量をマージする新しいスキームを提案した。2 つのスマートホームオープンデータセットに提案手法を適用し、行動認識精度を高く（87.3～94.62%）に維持しながら、再識別確率を、大幅に低下（100%から、73.85%～41.18%に低下）させることに成功した。

全体として、本論文は、差分プライバシに、特徴併合匿名化（FMA）という新規に考案したスキームを組み合わせることによって、スマートホームデータに対する、これまでに無い実用的なプライバシー保護を実現しており、本分野において十分な学術的新規性を有していることを確認した。以上より、本論文は、博士（工学）の学位論文として価値あるものと認める。