IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 14 March 2024, accepted 5 April 2024, date of publication 16 April 2024, date of current version 26 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3390039

RESEARCH ARTICLE

Preserving Data Utility in Differentially Private Smart Home Data

SOPICHA STIRAPONGSASUTI[1], FRANCIS JEROME TIAUSAS[1], YUGO NAKAMURA[2], (Member, IEEE), AND KEIICHI YASUMOTO[1,3], (Member, IEEE)

[1]Nara Institute of Science and Technology, Ikoma, Nara 630-0192, Japan
[2]Department of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819-0395, Japan
[3]RIKEN Center for Advanced Intelligence Project AIP, Tokyo 103-0027, Japan

Corresponding author: Sopicha Stirapongsasuti (stirapongsasuti.sopicha.so9@is.naist.jp)

This work was supported in part by JSPS KAKENHI under Grant JP21H03431 and Grant JP19H05665.

ABSTRACT The development of smart sensors and appliances can provide a lot of services. Nevertheless, the act of aggregating data containing sensitive information related to privacy in a single location poses significant issues. Such information can be misused by a malicious attacker. Also, some previous studies attempted to apply privacy mechanisms, but they decreased data utility. In this paper, we propose privacy protection mechanisms to preserve privacy-sensitive sensor data generated in a smart home. We leverage Rényi differential privacy (RDP) to preserve privacy. However, the preliminary result showed that using only RDP still significantly decreases the utility of data. Thus, a novel scheme called feature merging anonymization (FMA) is proposed to preserve privacy while maintaining data utility by merging feature dataframes of the same activities from other homes. Also, the expected trade-off is defined so that data utility should be greater than the privacy preserved. To evaluate the proposed techniques, we define privacy preservation and data utility as inverse accuracy of person identification (PI) and accuracy of activity recognition (AR), respectively. We trained the AR and PI models for two cases with and without FMA, using 2 smart-home open datasets i.e. the HIS and Toyota dataset. As a result, we could lower the accuracy of PI in the HIS and Toyota dataset to 73.85% and 41.18% with FMA respectively compared to 100% without FMA, while maintaining the accuracy of AR at 94.62% and 87.3% with FMA compared to 98.58% and 89.28% without FMA in the HIS and Toyota dataset, respectively. Another experiment was conducted to explore the feasibility of implementing FMA in a local server by partially merging frames of the original activity with frames of other activities at different merging ratios. The results show that the local server can still satisfy the expected trade-off at some ratios.

INDEX TERMS Differential privacy, machine learning, privacy, smart home.

I. INTRODUCTION

Thanks to developments of smart appliances/sensors in smart homes, smart services that can support dwellers such as lifelogging [1], [2], elderly monitoring [3], [4], appliances control [5], [6], anomaly detection [7], [8], etc. are proposed. To realize such services, a service provider (SP) needs to collect data from smart appliances/sensors where smart-home clients transfer the data to a cloud server(s), and the cloud server processes and analyzes the data by machine learning (ML) techniques. Since some data contain privacy-sensitive contents of dwellers [9], it is risky for them if an attacker could access the cloud server and use the data for malicious purposes. For instance, an attacker may use some techniques, e.g., ML, to re-identify a user for tracking activities of daily living (ADLs). Hence, it is essential to preserve user privacy in smart homes.

However, there are a lot of possible scenarios that could occur for privacy attacks and re-identification. For example, if we consider scenarios of privacy threats between an adversary and non-adversary, an adversary may eavesdrop on wireless communication of smart devices even if it

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

is encrypted traffic [10] and impersonate a target user to monitor and control, including aggregating some privacy-sensitive information [11]. Leitao's study [12] showed that malicious use of smart technologies as the context of intimate partner abuse could cause some users' high stress and anxiety. Therefore, solutions for solving the leakage of privacy-sensitive information are necessary to increase trustworthiness between users and smart sensors/appliances provided by the SP.

The aforementioned studies are mostly based on user perspectives. Some privacy attacks occur at a cloud server(s), which is one of the SP's parts, and most users may not realize it. However, the SP cannot provide good service quality if they apply privacy preservation methods because most of them can decrease data utility. This motivates us to find solutions to preserve privacy-sensitive data generated in a smart home while maintaining utility. However, there are some challenges to resolve, such as defining a trade-off between privacy preservation and data utility, applying differential privacy to smart home data, and achieving an expected trade-off between privacy preservation and utility.

In addition, the privacy preservation technique is the most challenging part. Since several sensors/appliances exist in a smart home, it is important to select proper techniques which can decrease the chance of privacy leakage from adversaries. According to existing studies, encryption cannot preserve data as it can be eavesdropped through network traffic. Therefore, other privacy preservation techniques have been proposed to preserve privacy in data, namely privacy preservation data mining (PPDM) [13], e.g., anonymization, perturbation, etc. Differential privacy (DP) [14] is a widespread PPDM technique to preserve data, especially in ML, because it has a low computational time and can decrease the likelihood that ML can predict by using random sampling distribution to generate synthetic (noise) data. However, DP has limitations, i.e., lack of standardization and agreement as it depends on data, algorithms, and techniques. Moreover, the synthetic data reduces the utility. Thus, the key challenge in DP is how to maintain the utility of data, such as the accuracy of recognition.

In [15], a privacy-aware data management method that controls data type and upload frequency for smart homes is proposed. However, the system has the limitation of potentially reducing the amount of uploaded data (to preserve privacy) which, in turn, may decrease the service performance that smart-home users could receive.

In this paper, we propose a privacy mechanism using DP to ensure all uploaded data in a smart home can be protected. To clarify, DP can be an alternative technique that we deploy to make the upload of data more secure. Although, as described before, DP can ensure data is preserved using sampling distributed noise, the accuracy of service, i.e., activity recognition, can decrease based on the privacy budget (ϵ) used. Hence, the proposed method leverages Rényi differential privacy (RDP) [16], which is approximate differential privacy, to provide lower privacy budgets for high-dimensional data. To know the effectiveness of RDP, we conducted a preliminary analysis of data on surveillance cameras from 2 smart home open datasets, namely the Health Smart Home (HIS) dataset [17] and Toyota Smart Home dataset [18], [19], which contains 15 homes. Unfortunately, the results of applying RDP to data and training with SVM showed that the recognition accuracy (utility) decreased much and home (user) identification accuracy did not decrease very much compared with the case without applying RDP. To overcome the problem, we define an expected trade-off so that data utility should be greater than the privacy preserved and propose a novel technique to secure video data, called feature merging anonymization (FMA). FMA applies the fundamental knowledge of k-anonymity by mapping video frames of the same activities performed by others prepared in advance.

We conducted an experiment where we trained the accuracy of activity recognition (AR) and person identification (PI) models for two cases with and without FMA, using the HIS dataset [17] and Toyota dataset [18], [19]. We defined privacy preservation and data utility as inverse accuracy of PI and accuracy of AR, respectively

The results of the simulation show that we could lower the accuracy of PI in the HIS and Toyota dataset to 73.85% and 41.18% with FMA respectively compared to 100% without FMA, while maintaining the accuracy of AR at 94.62% and 87.3% with FMA compared to 98.58% and 89.28% without FMA in the HIS and Toyota dataset, respectively. Another experiment is conducted to prove if the proposed method is feasible in a practical environment by applying FMA with mixed activities, the same activity and other activities at a certain ratio: from 1:0 to 0.5:0.5. The results show that the expected trade-off can still be achieved at some ratios.

Our contributions are the following:

- We proposed a threat model which an adversary can illegally access an untrusted cloud of a service provider and identify smart home users by mapping eavesdropped data to identified homes.
- We proposed a novel privacy preservation technique called feature merging anonymization (FMA), which merges the data of the same activity by other homes, and showed that FMA can achieve the expected trade-off.

II. RELATED WORK

A. PRIVACY PRESERVATION TECHNIQUE

Since a lot of privacy preservation techniques [18], [19], [20], [21] have been proposed for the smart home system such as using heuristic-based techniques to modify the selected values to minimize the effectiveness loss, encryption techniques [22], [23], [24] to preserve privacy for computation, and reconstruction-based techniques to reassembled data randomly. However, these techniques cannot protect data leakage if an attacker uses ML. Because the original data which contains privacy-sensitive data is not modified. Therefore, the privacy preservation technique in this subsection

focuses on reconstruction-based techniques also known as privacy preservation data mining (PPDM) and it can be categorized into 4 techniques, i.e., anonymization [25], perturbation [26], randomized response [27], condensation [28]. However, anonymization is the most known technique due to its capability of preserving the sensitive attributes of data records by making them indistinguishable. The most prevalent mechanism is k-anonymity [29], [30] which can guarantee that the data is indistinguishable from at least 1-k records. Many smart home systems applied the k-anonymity for big data queries generated from appliances/sensors [31], [32], [33], [34]. Other anonymization mechanisms are also leveraged to secure a smart home, e.g. l-diversity [35], publishing the trajectories [36], normalization [37], etc. In recent years, differential privacy (DP) [38] has become widespread. Since it can preserve high-dimensional sensitive data, it is leveraged to protect privacy-sensitive data used in ML, especially in neural networks (NN) [39], [40], [41].

B. RELATED PRIVACY MECHANISM: DIFFERENTIAL PRIVACY

Definition 1: Differential privacy (DP). A randomized algorithm $F : D \rightarrow D'$ provides ϵ-differential privacy (ϵ-DP) if for every pair of neighboring inputs $d, d' \in D$, and for every (measurable) set $\phi \subseteq D'$, the probabilities of events $F(d) \in \phi$ and $F(d') \in \phi$ are closer than a factor of $exp(\epsilon)$:

$$Pr[F(d) \in \phi] \leq exp(\epsilon) Pr[F(d') \in \phi] \tag{1}$$

where ϵ denotes the privacy budget to make $F(d)$ satisfy ϵ-differential privacy. Also, the randomized function F the Laplace mechanism defined as follows:

$$F(d) = f(d) + Lap(\frac{s}{\epsilon}) \tag{2}$$

where s is the L1-sensitivity of function f and $Lap(\frac{s}{\epsilon})$ is the sampling function from Laplace distribution. In addition, the local sensitivity s can be calculated from the maximum distance between $F(d)$ and $F(d')$ as follows:

$$s = \max_{dist(d,d') \leq 1} |F(d) - F(d')| \tag{3}$$

where $dist(d, d')$ denotes the distance between 2 neighboring data. Instead of using Laplace distribution, another mechanism uses Gaussian distribution. This mechanism can satisfy (ϵ, δ)-differential privacy, which is the approximate differential privacy. Let δ denote a failure probability, and the sensitivity s used in the Gaussian mechanism to be the L2-sensitivity. Then, from eq.1, (ϵ, δ)-differential privacy can be derived as:

$$Pr[F(d) \in \phi] \leq exp(\epsilon) Pr[F(d') \in \phi] + \delta \tag{4}$$

Let $\sigma = \frac{2slog(1.25/\delta)}{\epsilon^2}$. Then, the Gaussian mechanism is defined as follows:

$$F(d) = f(d) + \mathcal{N}(\sigma^2) \tag{5}$$

In addition, DP can be defined as the term of max divergence, where divergence is a statistical method to measure distance based on two probability distributions. The Kullback-Leibler divergence [42] is defined as:

$$D_{KL}(P||Q) = \sum_{d \in D} P(d \in D) \left[log \frac{P(d \in D)}{Q(d \in D)} \right] \tag{6}$$

Hence, the max divergence between two probability distributions can be defined as:

$$D_{\infty}(P||Q) = \max_{d \in D} \left[log \frac{P(d \in D)}{Q(d \in D)} \right] \tag{7}$$

From eq. 1 and 7, F satisfies ϵ-differential privacy if:

$$D_{\infty}(F(d)||F'(d)) \leq \epsilon \tag{8}$$

Rényi differential privacy (RDP) [16] is a relaxation of (ϵ, δ)-differential privacy that applies the Gaussian mechanism and the characteristics of max divergence. The Gaussian mechanism in RDP is the same as eq. 5 but $\sigma^2 = \frac{\Delta f^2 2\alpha}{2\overline{\epsilon}}$, where α is the order of the Rényi divergence. Let $\overline{\epsilon} = \epsilon - \frac{log(1/\delta)}{\alpha - 1}$, then the function F satisfies $(\alpha, \overline{\epsilon})$-differential privacy as follows:

$$D_{\infty}(F(d)||F'(d)) \leq \overline{\epsilon} \tag{9}$$

According to the definition of $\overline{\epsilon}$, F in RDP also satisfies (ϵ, δ)-differential privacy if $\delta > 0$ and α can be scaled from 2 to 100. The advantage of using RDP is that it can decrease the privacy budget ϵ for high-dimensional data compared to the original ϵ-differential privacy. This is because it provides a tighter composition property, which results in a lower privacy budget when applying the mechanism sequentially.

In our research, the simulation experiment deploys data from multiple cameras in 2 public smart home datasets that contains more than 30,000 frames. Thus, RDP can decrease the privacy budget ϵ used in this dataset by applying noise function $\mathcal{N}(\sigma^2)$ based on RDP to each smart home dataframes.

C. PRIVACY AND UTILITY TRADE-OFF

As mentioned in the introduction, preserving private data can decrease the usability of data to generate services from SP to promote smart living in a home. Thus, there have been a lot of efforts to solve the privacy and utility trade-off. For example, Chang et al. [43] performed the multi-objective optimization problem for the trade-off between energy cost and privacy. They defined privacy leakage from the energy consumption pattern while the ideal privacy preservation occurs when the power consumption is time-invariant. Hence, privacy can be minimized. Bi et al. [44] present a privacy isolation zone to provide privacy on gait information generated from accelerometers using high-pass and low pass filter before uploading to a cloud end and process a security module by the CNN. To preserve visual privacy-sensitive data, Wang et al. [41] used a lower image sensor resolution technique and constructed a model for calculating the trade-off between visual privacy-preserving and activity recognition. The result of optimization shows that a resolution between 20 × 20 and

30×30 can indicate a proper resolution for balancing privacy preservation and activity recognition. However, lower image sensor resolution might decrease utility data such as activity recognition accuracy for some micro activities. Erdemir et al. [45] proposed a method to let users actively choose from among a finite number of data release mechanisms (DRMs) i.e., conditional probability distributions at each time to reveal their data and get utility in return. Although the evaluation of the results could satisfy privacy and utility trade-off, the decision-making method seems impractical due to real-time decisions by users. Malekzadeh et al. [46] presented privacy preservation techniques, namely the replacement auto encoder (RAE) to protect sensitive inferences and an anonymizing auto encoder (AAE) to prevent user re-identification. Even though these could preserve privacy data on the user side, utility data might decrease if there's a lot of sensitive data generated.

Recently, there have been a lot of attempts to achieve privacy and utility trade-off using DP. For instance, Cao et al. [47] deployed DP to generate noise into feature data and its evaluation result could achieve privacy preservation better than applying DP to raw data. Zhang et al. [48] presented a differential privacy model namely, attack-proof personalized differential privacy (APDP). The model uses fog computing for DP integrated with the Markov process to resist collusion attacks. They compared APDP with 2 privacy models and evaluated the privacy trade-off with root-mean-square error. The results showed that APDP used a lower privacy budget (ϵ) and reflected higher utility data than the others. The limitation of the model is that it can increase utility data when it has multiple clouds. Qashlan et al. [49] presented DP schemes with blockchain. Their experiment applied RDP to 3 datasets and found the optimal privacy budget $\epsilon = 10^{-1}$ for the best trade-off. However, it cannot represent the optimal privacy budget for other datasets due to the inherent correlation between data points. Hassan et al. [50] leveraged Gaussian Noise Differential Privacy (GNDP) with peak value protection to smart meter data and provided a trade-off with the error rate. Results from an experiment demonstrated the best privacy preservation at a peak value of 1200 Wh. having only a 1.5% error. A similar study was conducted by Wang et al. [51]. They proposed a privacy framework, namely PrivStream by applying encoder-decoder filter and DP to accelerometer, attitude, and gyroscope data. However, it is difficult to apply such a method in high-dimensional data. Hence, Wang et al. [39] proposed a privacy preservation technique using DP to RGB pixels of video data and showed a good result in terms of re-identificaction accuracy. Since the experiment was conducted with 3 small datasets, which their frames are not over 1200 frames, computational time and memory consumption would increase in bigger datasets. Mao et al. [52] focused on privacy leakage through split learning of deep neural networks (SplitNN). Thus, they presented a privacy-preserving method for image classification with a new activation function, namely R3eLU. Nevertheless, the solution still remains some privacy issues such as label leakage.

Previous studies have shown that it is challenging to find a good trade-off between the privacy and utility of applications for smart home or time series data. In addition, most smart home data used in ML are generated from smart appliances/sensors due to privacy concerns. However, in real-world situations, most smart-home users attach surveillance cameras to secure their homes or to monitor elderly people or babies. Since video data contain highly privacy-sensitive data, to the best of our knowledge, few studies provide solutions to maintain an optimal privacy and utility trade-off. This motivates and challenges us to conduct the research in order to achieve the balance while considering a lot of factors e.g. servers, data, resources, and so on to form a smart home having trustworthiness between smart home residents and SP.

III. RESEARCH PROBLEMS

We define two research questions that should be addressed.

RQ1: HOW TO QUANTIFY THE TRADE-OFF BETWEEN PRIVACY PRESERVATION AND UTILITY?

In this study, we regard the trade-off between privacy preservation and data utility as the trade-off between the inverse accuracy of person identification (PI) and accuracy of activity recognition (AR). To answer RQ1, we utilize the video data from surveillance cameras from a smart home dataset for analysis and simulation experiments. Moreover, the smart home data is distributed to each timeslot based on timestamps recorded in the annotation file. The reason for using timeslot-based data is that an adversary is assumed to eavesdrop on smart home data during some time slots.

RQ2: HOW TO INCREASE DATA UTILITY WHEN APPLYING PRIVACY TECHNIQUES?

When DP is applied to high-dimensional data, it will be done in a sequential manner, leading to increased ϵ values. Since the video data contains multiple arrays of sequential frames, we use Rényi differential privacy (RDP) to address this problem. Because it is derived from Gaussian distribution and max-divergence mechanisms, which is explained in section IV, it can decrease the ϵ used for the dimensional data and provide the α value to vary the accuracy of PI.

Since the characteristics of DP, including RDP, can preserve the privacy of smart home data based on the sampling distribution of noise, this can imply that the accuracy of AR can still be lower than that of PI. Thus, we set the expected trade-off between privacy preservation and data utility so that the accuracy of AR should be higher than PI. To satisfy the expected trade-off, we propose feature merging anonymization (FMA) in Sect. IV, which can decrease the possibility of being identified by the ML model while maintaining the utility of recognizing data.

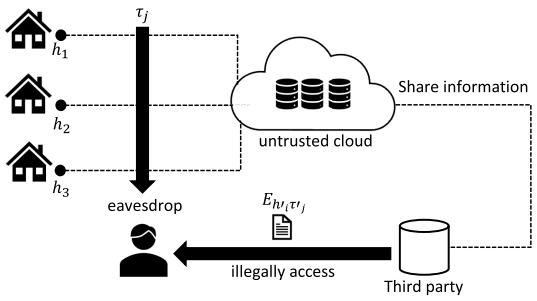

FIGURE 1. Threat model shows the adversary can eavesdrop smart home data and illegally acquire data from a third party.

IV. PROPOSED PRIVACY PRESERVATION TECHNIQUE

In this section, after we provide the assumed threat model, we describe the DP-based privacy preservation method for smart home data. Then, we propose a novel privacy preservation method called feature merging anonymity (FMA).

A. THREAT MODEL

Due to our assumptions on an untrusted cloud server, a malicious attacker has the ability to access the cloud server to acquire data, as shown in Fig.1. Moreover, the attacker has the potential to illegally access some homes or all homes to monitor the event set of some smart homes by eavesdropping. However, they can eavesdrop on the set for some time in a day. Also, we assume that the attacker can receive information about the number of identified homes based on membership inference attacks [53]. The attacker queries the target model with a data record and obtains the model's prediction on that record, which is a vector of probabilities, one per class, that the record belongs to a certain class. The attacker tries to distinguish each home from the others by mapping eavesdropped data and the identified home to know which smart home data corresponds to the identified home. Therefore, our goal is to apply DP to make homes indistinguishable at local servers and data of homes in each timeslot is prepared in advance and shared among homes.

B. FEATURE MERGING ANONYMIZATION FOR SECURE VIDEO DATA

We newly propose a privacy mechanism called Feature Merging Anonymization (FMA), which has a similar idea to k-anonymity, but the anonymization will be done in terms of features generated from frames. Since the video data contains a lot of sequential frames that can easily be identified, using only DP to achieve privacy data preservation can significantly decrease the utility [54]. Hence, this method is used to maintain the utility of feature data and decrease the possibility of identifying users.

Definition 2: Feature Merging Anonymity (FMA). Let X and Y denote two-dimensional binary arrays corresponding to video feature frames, respectively. Let n be an integer number. Feature Merging Anonymization (FMA) is a function $FMA(X, Y, n)$, which merges each frame of X with n frames randomly selected from Y, allowing for duplicates. Here, the merging operation of two frames is a bitwise OR operation.

Let $X_{h,a}$ be a set of binary encoding frames of a user performing an activity a in a home $h \in H$ and $Y_{h',a}$ be a set of frames of other homes $h' \in H'$ performing the same activity a. We apply FMA to $X'_{h,a}$ and obtain a new set of frames $X'_{h,a}$ as following:

$$X'_{h,a} = FMA(X_{h,a}, Y_{h',a}, n), \quad \forall x \in X, \exists y \in Y \tag{10}$$

To apply such a method to smart home data of multiple homes, each room in the home area is assumed to have the same environment and layout, e.g., an apartment. The video surveillance cameras of each home are managed by the service provider with the same angle.

The preliminary analysis result in the section V shows the effect of FMA on video data recorded in smart homes. We assume that for each activity, the video data for the activity performed by other people with the same layout is prepared by the service provider and provided to each home. We also assume that the video data corresponding to the current activity can be retrieved with 100% of accuracy. This assumption will be loosened later.

C. THE EXPECTED TRADE-OFF

Let $AR(X_{H,T})$ and $PI(X_{H,T})$ be the average accuracy of activity recognition (AR) and person identification (PI) for all homes H and all time slots T, respectively. Hence, we set the expected trade-off between AR and PI as follows:

$$AR(X_{H,T}) - PI(X_{H,T}) > 0 \tag{11}$$

This trade-off means that AR must be greater than PI. A similar assumption can be found in [41], which is the trade-off between activity recognition and privacy preservation using pixelation.

V. PRELIMINARY ANALYSIS

In this section, we describe the analysis of 2 public smart home datasets, namely the Health Smart Home (HIS) dataset [17] and Toyota Smart Home dataset [55], [56]. There are 15 homes with sensor/appliance data and video data from surveillance cameras in the HIS dataset. While the Toyota dataset has 18 homes with video data from surveillance cameras. We apply privacy preservation techniques to the video data because, recently, most smart homes use the surveillance cameras to prevent physical security attacks, e.g., thefts, unaccounted visitors, stalkers, and so on. As this data contains privacy-sensitive data such as residents' faces and activities, it is essential to preserve privacy in such data. Hence, this analysis aims to evaluate the trade-off between the accuracy of AR and PI of the original dataset before applying privacy mechanisms for an experiment.

A. DATA PRE-PROCESSING

1) HIS DATASET

Each home data in the HIS dataset contains the data of four surveillance cameras compressed in MPEG 4 (Xvid codec)

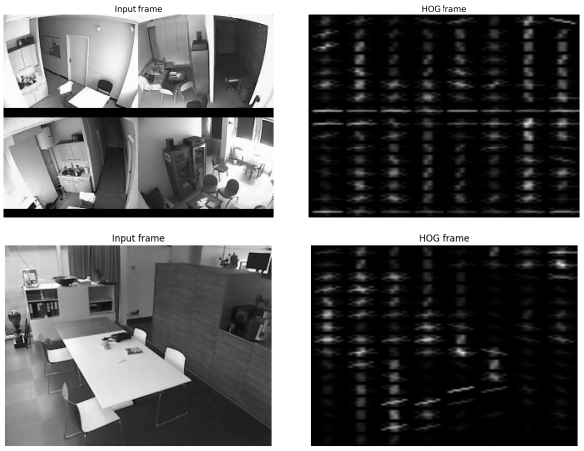

FIGURE 2. Samples of original frames and HOG frames from the HIS dataset (upper row) and Toyota dataset (lower row).

in a frame. The four cameras are located in the kitchen on the top left, between the kitchen, hall, and bathroom door on the bottom left, the bedroom and living room on the top right, and the living room only on the bottom right, respectively, as shown in Fig. 2 (upper row left). There are 7 activities recorded, i.e., sleeping, resting (watching TV, reading, listening to a radio, ...), dressing/undressing, eating, using the toilet, performing hygiene, and communicating. According to the threat model described in Sect. IV-A, the attacker(s) is capable of eavesdropping smart home data for some time slots. Thus, we sampled 1-second frames from 15-fps video data of each home using the OpenCV library for binary encoding as grey scales (0–255). The frame's resolution is set to 64 × 128 before applying the histogram of oriented gradients (HOG) feature. The number of frames of each home data is presented in Table 1. The data was divided into 24 timeslots (1 hour per slot) based on the video timestamps from the annotation files. Since we found that the data exist only in 8-th, 9-th, 10-th, 11-th, 12-th, 14-th, 15-th, 16-th and 17-th timeslots. Furthermore, there are not more than five homes belonging to all timeslots. Due to the imbalance of data distribution, it is difficult to evaluate the proposed method with timeslot-based data for person identification and activity recognition. Therefore, we split all data in each home into 24 chunks and distributed them to 24 timeslots.

2) TOYOTA DATASET

The Toyota dataset has 536 video files from all participants. Each video has a single camera in a frame. The number of frames of each home data is presented in Table 2 . There are 51 activities recorded, but we combined micro activities to reduce the amount to 30 activities for classification. Samples of video frames are shown in Fig. 2 (lower row left). We divided the data into 25 timeslots based on video labels and selected 21 timeslots due to the appearance of multiple homes ($N \geq 2$). The process of generating data before applying the HOG feature was the same way in the HIS dataset, but the data sampling was at every 600 frames from 20-fps video data.

B. FEATURE EXTRACTION

Before implementing RDP, we generated a feature for the video data using the histogram of oriented gradients (HOG) feature [57]. This feature is well known for object detection and human recognition. Since the HOG feature calculates the magnitude and direction of the gradients at each pixel of an input frame, we empirically set 9, 8 × 8, and 2 × 2 to orientations, the number of pixels per cell, and cell size per block of each frame for calculating the HOG feature. Fig. 2 illustrates an input image frames (left) and HOG feature frames (right) from both datasets. We can see that the orientations of HOG depend on the environment in the image i.e. the HOG orientations can represent the dark area or high intensity area better than the lower one.

C. SENSITIVITY OF RAW DATA

Due to DP mechanisms, the sensitivity needs to be calculated from the maximum distance of neighboring data as explained in section IV. Hence, L2 distance is employed as the method to calculate distance. To do so, we calculated the summation of binary encoded pixels of all HOG frames of all homes in all timeslots. Then, we selected the maximum summation of the HOG frame for each home and calculated the L2 distance among homes. The results of the maximum distance averaged from all time slots in HIS dataset and Toyota dataset are 1913.07 and 1472.62, respectively, which represent the sensitivity of HOG frame data.

D. APPLYING RÉNYI DIFFERENTIAL PRIVACY (RDP)

We trained the model using the original dataset extracted by the HOG feature without implementing RDP as the baseline. The data was split into two portions: 70% for training and 30% for testing. Since the video data contains pixel arrays that can be linearly separable, we used linear SVM as a training model for both activity recognition and person identification. The model is evaluated by one-vs-the-rest (OvR) multiclass classification.

The results of the accuracy of AR and PI without implementing any privacy preservation techniques on the HIS and Toyota dataset are shown in Table 3 . We can see that the accuracy of the AR of the HIS dataset is higher than the Toyota dataset, while the accuracy of the PI of both datasets is equal to 100%.

To generate synthetic data from RDP, we set the privacy budget $\bar{\epsilon}$ at 1.1 (ln3), 3, 5 and α at 2, 20, 40 for analysis. Fig. 3 presents synthetic images and HOG images of $\bar{\epsilon} = 1.1$ (ln3), 3, 5 at different α values in order. The smaller $\bar{\epsilon}$ is, the more privacy is preserved. On the other hand, the greater α is, the more privacy is preserved.

Fig. 4 demonstrates the results after applying RDP with different pairs of $(\bar{\epsilon}, \alpha)$ to both datasets We can see that the accuracy of AR is still lower than PI for all pairs of $(\bar{\epsilon}, \alpha)$.

TABLE 1. The amount of frames in each home in the HIS dataset.

Home no.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Amount of frames	6916	5331	2770	6694	863	2888	2775	3329	3978	3580	3721	324	1931	2527	4369

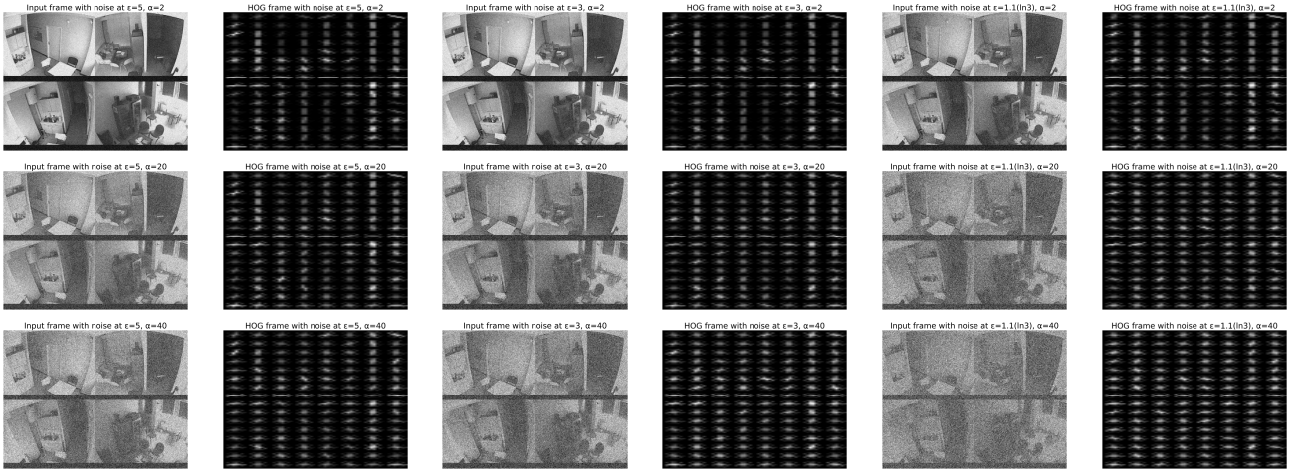

FIGURE 3. Synthetic images and HOG images in the HIS dataset at different $\bar{\epsilon}$ i.e. 5, 3, 1.1 (ln3) (from left to right) and $\alpha = 2, 20, 40$ (from top to bottom).

TABLE 2. The amount of frames in each home in the Toyota dataset.

Home no.	Amount of frames
2	535210
3	770141
4	845449
6	929387
7	937587
9	823690
10	675908
11	495479
12	522676
13	654582
14	764380
15	910813
16	803258
17	796152
18	756193
19	604983
20	699040
25	884298

This can confirm that using RDP, which is the approximate DP, still greatly decreases the utility of activity recognition when trying to decrease the person identification probability.

VI. SIMULATION EXPERIMENT

In this section, we describe how to apply FMA to make a better trade-off between AR and PI. We conducted two simulation experiments to apply FMA: (1) merging with the same activity frames performed by other homes and (2) merging with the same activity frames and other activity frames performed by other homes in some different ratios.

A. SIMULATION EXPERIMENT I: MERGING WITH THE SAME ACTIVITY FRAMES

The purpose is to confirm if FMA can satisfy the expected trade-off. In this experiment, we assume that for each home, video frames of all activities in each time slot performed by other homes are prepared in advance and shared with the home (ideally, activities performed by third-party homes would be prepared and shared). FMA will generate the frame data of each smart home as explained in Sect. IV-B.

TABLE 3. The accuracy of activity recognition and person identification from HIS dataset and Toyota dataset.

Dataset	Activity recognition	Person identification
HIS	98.58%	100%
Toyota	89.93%	100%

Since merging for video feature frames needs a proper ratio to achieve the best trade-off, we conducted an experiment by assigning different ratios of merging other home frames to the original frames (i.e., original frames: other home frames) in each timeslot from 0.5:0.5 to 0.05:0.95. For example, suppose that a sleeping activity of user A was recorded from 23:00 to 7:00. In this case, the local server of user A will randomly merge each video frame of the sleeping activity of user A with those of sleeping activity performed by other homes. Because we set a certain ratio of merging, the outputs are video feature frames of the sleeping activity from user A and other homes. Also, we used the RDP at $\bar{\epsilon} = 5$ and $\alpha = 2$, which is a low noise sampling to observe the effect of FMA on the accuracy of AR and PI.

The result of applying RDP and FMA at different ratios is shown in Fig. 5. Since we implemented RDP at $\bar{\epsilon} = 5, \alpha = 2$, AR of the HIS and Toyota dataset remain at approximately 95%, 87% of the accuracy, respectively, while PI tends to decrease at different ratios. The results of PI in the Toyota dataset decrease significantly compared to the HIS dataset due to the larger number of frames and various activities in each timeslot. The ratio of merging frames at 0.05:0.95 can achieve the best trade-off.

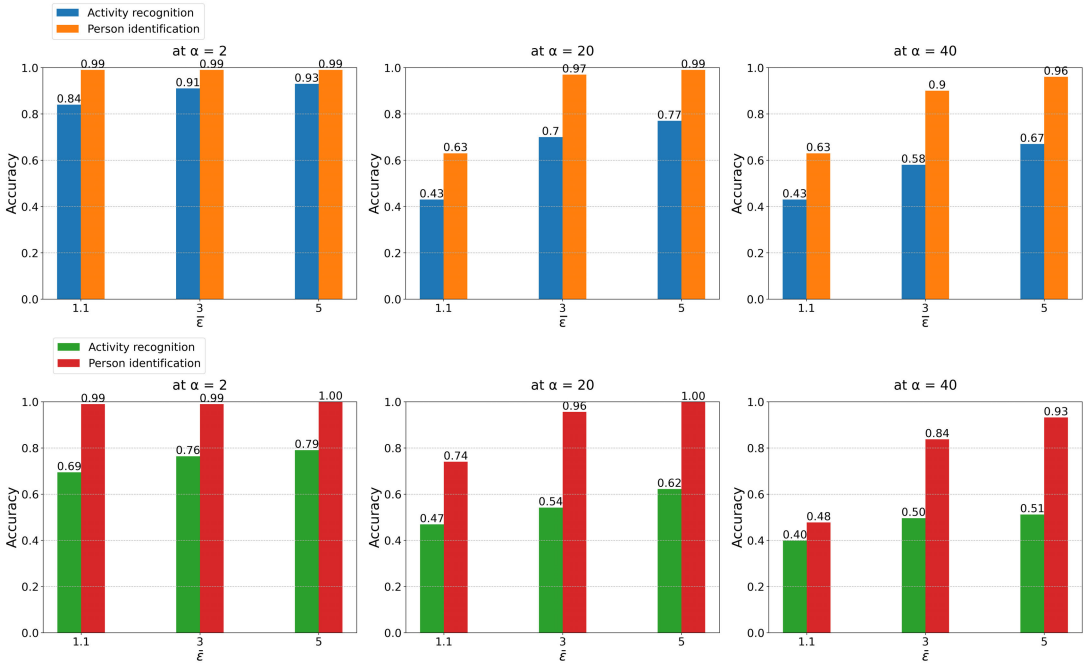

FIGURE 4. The accuracy of activity recognition and person identification of the HIS (upper row) and Toyota dataset (lower row) at different $\overline{\epsilon}$ i.e. 1.1 (ln3), 3, 5 with $\alpha = 2, 20, 40$ from left to right.

After we found that the best ratio of merging frames is at 0.05:0.95, we set privacy budget $\overline{\epsilon}$ at 1.1 (ln3), 3, 5 and α at 2, 20, 40 for training RDP with FMA which is the same values as the method in section V for comparison. The results of the experiment using RDP with FMA at different pairs of $(\overline{\epsilon}, \alpha)$ are shown in Fig. 6. We can see that our proposed privacy mechanisms provide a better trade-off compared to the results in section V (Fig. 4). At $\alpha = 2$, the accuracy of AR for all $\overline{\epsilon}$ values are higher than the accuracy of PI by 18% and 44% on average in the HIS and Toyota dataset respectively. Between AR and PI in the HIS dataset at $\alpha = 20$, the expected trade-off is satisfied only when $\overline{\epsilon} = 3$ and 5. At $\alpha = 40$, only $\overline{\epsilon} = 5$ can satisfy the expected trade-off. While the accuracy of AR in the Toyota dataset is higher than PI for all pairs and increases 19.78% on average. In addition, when we compare the result to the previous one (Fig. 4), which used only RDP, we can see that the accuracy of PI in both datasets significantly decreases at each pair $(\overline{\epsilon}, \alpha)$.

B. SIMULATION EXPERIMENT II: PARTIALLY MERGING WITH OTHER ACTIVITIES

The purpose of this experiment is to show that even if the local server cannot precisely predict the uploading activity, and is therefore forced to merge with approximately the same activity performed by other homes, the combination of FMA and RDP can still provide the expected trade-off. Hence, we applied the different merging ratio of the same activity to other activities by other homes in each timeslot.

We set the ratio of merging the same activity with other activities from 1:0 to 0.5:0.5. To clarify, we provide an example of partially merging with other activities: a sleeping activity of user A was recorded from 23:00 to 7:00. In this case, the local server of the user A will randomly merge each video frame of sleeping activity of user A with sleeping and other activities performed by other homes (with a certain ratio) for each one hour timeslot (from 23:00 to 7:00). The merging outputs are video frames of the sleeping activity from user A which partially contains the same activity and other activities from other homes.

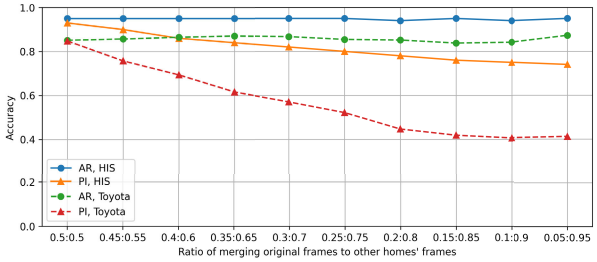

FIGURE 5. The result of RDP at $\overline{\epsilon} = 5$, $\alpha = 2$ with FMA at different ratios of merging third-party frames to original frames.

In Fig. 7, each graph demonstrates the accuracy of AR and PI when merging ratios of the same activity to other activities at different ratios of merging the original frames to other homes' frames in both datasets. The graph in the top left corner is the ideal result because the merging ratio = 1:0 means merging with the same activity for all homes. Furthermore, we can see that PI decreases when the ratio of merging with other activities increases, while AR is still higher than PI in most cases. PI becomes the lowest when the merging ratio of the original frame to another activity frame is 0.5:0.5 and PI results in the Toyota dataset are lower than ones in the HIS dataset for all ratios. Based on these results, we can confirm that our privacy preservation method can still

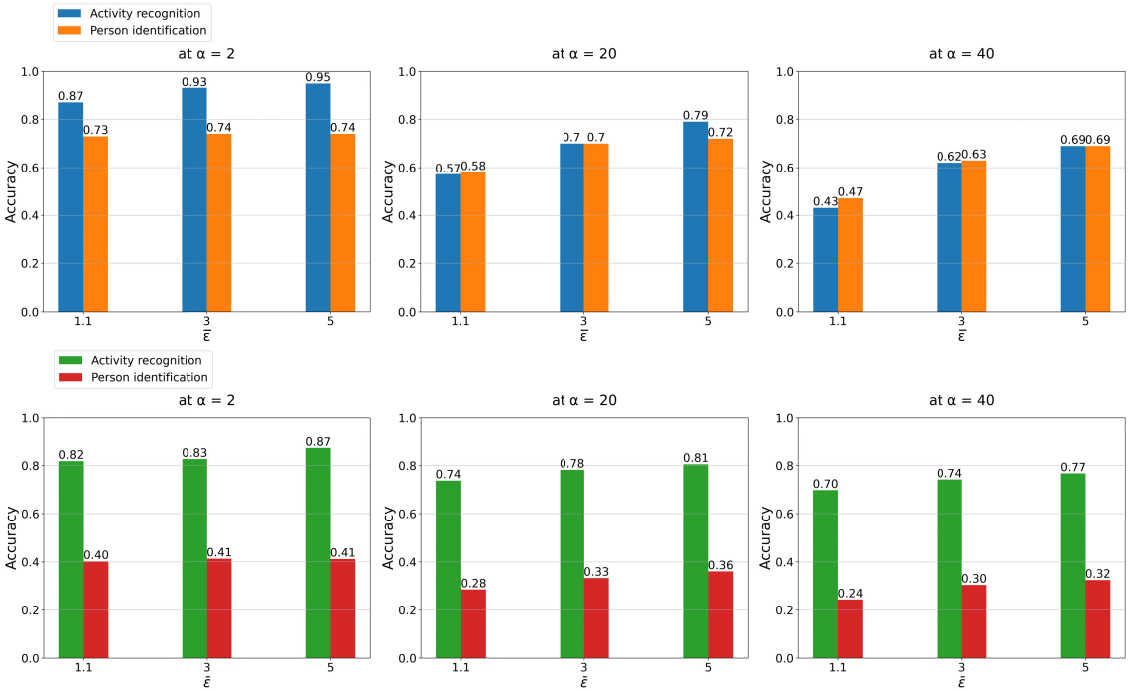

FIGURE 6. The accuracy of activity recognition and person identification of the HIS (upper row) and Toyota dataset (lower row) at different $\bar{\epsilon}$ i.e. 1.1 (ln3), 3, 5 with $\alpha = 2$, 20, 40 and FMA at the ratio = 0.05:0.95 from left to right.

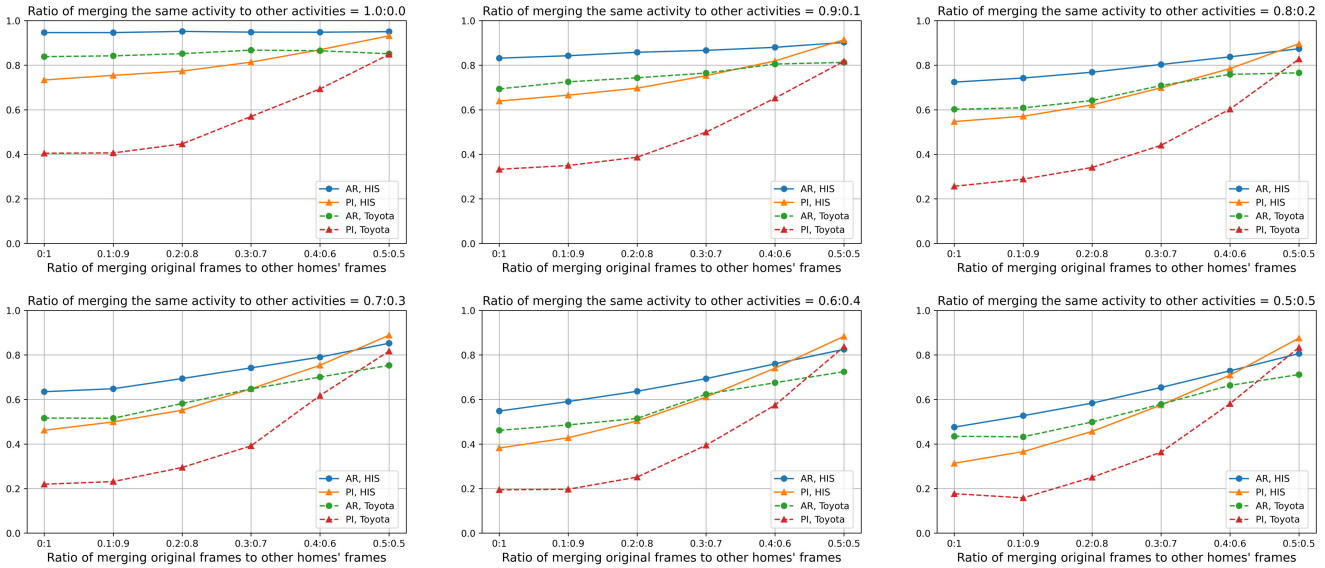

FIGURE 7. The accuracy of activity recognition and person identification at $\bar{\epsilon} = 5$, $\alpha = 2$ at different ratios of merging the same activity and other activities.

achieve the expected trade-off in most cases except merging other homes' frames 50% with other activity more than 20%.

VII. CONCLUSION

In this paper, we tried to preserve user's privacy in smart home video data while maintaining the data utility by leveraging RDP which is an approximate DP. We regarded the trade-off between privacy preservation and the utility of data as the trade-off between the accuracy of person identification (PI) and activity recognition (AR) to solve the research problem RQ1. Besides, the expected trade-off is proposed to be the solution of the research problem RQ2 which AR must be greater than PI. Through a preliminary analysis, we confirmed that only RDP cannot achieve the expected trade-off. Therefore, we devised a novel privacy mechanism, namely FMA to satisfy the expected trade-off between privacy preservation and data utility by merging the video frames of the same activity performed by other homes.

Using 2 public smart home video datasets, we conducted simulation experiments that trained dataframes using RDP

and merging the same activity frames with FMA. The results of the simulation showed that a good trade-off can be achieved when using a 0.05:0.95 ratio of merging third-party frames. This lowers the PI accuracy in the HIS and Toyota dataset to 73.85% and 41.18% respectively compared to 100% of the original video data, while keeping good AR accuracy of 94.62% and 87.3% compared to 98.58% and 89.28% for the original video data in the HIS and Toyota dataset respectively. Also, another simulation experiment was conducted to show if the expected trade-off still satisfies even though the local server cannot precisely predict the ongoing activity by partially merging with other activities. The experiment results showed that it can still satisfy the expected trade-off at some ratios.

Since the proposed privacy mechanism still has some limitations regarding data dependence such as size, distribution, and similarity of data, further data analysis to standardize the threshold of privacy trade-off is necessary. Also, the usability of our privacy preservation mechanism at decentralized servers such as edge servers should be further considered and analyzed if it can provide more secure smart home systems.

REFERENCES

[1] T. Matsui, S. Misaki, Y. Sato, M. Fujimoto, H. Suwa, and K. Yasumoto, "Multi-person daily activity recognition with non-contact sensors based on activity co-occurrence," in *Proc. 13th Int. Conf. Mobile Comput. Ubiquitous Netw. (ICMU)*, Nov. 2021, pp. 1–8.

[2] A. Jalal, S. Kamal, and D. Kim, "A depth video sensor-based life-logging human activity recognition system for elderly care in smart indoor environments," *Sensors*, vol. 14, no. 7, pp. 11735–11759, Jul. 2014.

[3] M. Yu, A. Rhuma, S. M. Naqvi, L. Wang, and J. Chambers, "A posture recognition-based fall detection system for monitoring an elderly person in a smart home environment," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1274–1286, Nov. 2012.

[4] M. J. Deen, "Information and communications technologies for elderly ubiquitous healthcare in a smart home," *Pers. Ubiquitous Comput.*, vol. 19, nos. 3–4, pp. 573–599, Jul. 2015.

[5] P. Kumar and U. C. Pati, "IoT based monitoring and control of appliances for smart home," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 1145–1150.

[6] F. Mehmood, I. Ullah, S. Ahmad, and D. Kim, "Object detection mechanism based on deep learning algorithm using embedded IoT devices for smart home appliances control in CoT," *J. Ambient Intell. Humanized Comput.*, vol. 10, pp. 1–17, Mar. 2019.

[7] U. Bakar, H. Ghayvat, S. F. Hasanm, and S. C. Mukhopadhyay, "Activity and anomaly detection in smart home: A survey," *Next Gener. Sensors Syst.*, vol. 16, pp. 191–220, Jul. 2015.

[8] M. Novak, M. Binas, and F. Jakab, "Unobtrusive anomaly detection in presence of elderly in a smart-home environment," in *Proc. ELEKTRO*, 2012, pp. 341–344.

[9] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[10] S. Kennedy, H. Li, C. Wang, H. Liu, B. Wang, and W. Sun, "I can hear your alexa: Voice command fingerprinting on smart home speakers," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 232–240.

[11] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2017, pp. 1292–1297.

[12] R. Leitão, "Anticipating smart home security and privacy threats with survivors of intimate partner abuse," in *Proc. Designing Interact. Syst. Conf.*, Jun. 2019, pp. 527–539.

[13] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, May 2000, pp. 439–450.

[14] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, Venice, Italy. Berlin, Germany: Springer, 2006, pp. 1–12.

[15] S. Stirapongsasuti, Y. Nakamura, and K. Yasumoto, "Privacy-aware sensor data upload management for securely receiving smart home services," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Sep. 2020, pp. 214–219.

[16] I. Mironov, "Renyi differential privacy," in *Proc. IEEE 30th Comput. Secur. Found. Symp. (CSF)*, Aug. 2017, pp. 263–275.

[17] A. Fleury, M. Vacher, and N. Noury, "SVM-based multimodal classification of activities of daily living in health smart homes: Sensors, algorithms, and first experimental results," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 2, pp. 274–283, Mar. 2010.

[18] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1501–1514, Nov. 2009.

[19] H. Vaghashia and A. Ganatra, "A survey: Privacy preservation techniques in data mining," *Int. J. Comput. Appl.*, vol. 119, no. 4, pp. 20–26, Jun. 2015.

[20] R. Mendes and J. P. Vilela, "Privacy-preserving data mining: Methods, metrics, and applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2017.

[21] P. R. M. Rao, S. M. Krishna, and A. P. S. Kumar, "Privacy preservation techniques in big data analytics: A survey," *J. Big Data*, vol. 5, no. 1, pp. 1–12, Dec. 2018.

[22] L. Kissner and D. Song, "Privacy-preserving set operations," in *Advances in Cryptology—CRYPTO*, Santa Barbara, CA, USA. Berlin, Germany: Springer, 2005, pp. 241–257.

[23] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017.

[24] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-Health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.

[25] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proc. 21st Int. Conf. Data Eng. (ICDE)*, 2005, pp. 217–228.

[26] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," in *Proc. 3rd IEEE Int. Conf. Data Mining*, Nov. 2003, pp. 99–106.

[27] W. Du and Z. Zhan, "Using randomized response techniques for privacy-preserving data mining," in *Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2003, pp. 505–510.

[28] C. C. Aggarwal and P. S. Yu, "A condensation approach to privacy preserving data mining," in *Proc. Int. Conf. Extending Database Technol.* Berlin, Germany: Springer, 2004, pp. 183–199.

[29] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: K-anonymity and its enforcement through generalization and suppression," Comput. Sci. Lab., SRI Int., CA, USA, Tech. Rep. SRI-CSL-98-04, 1998.

[30] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information," in *Proc. PODS*, vol. 98, 1998, p. 1145.

[31] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," *IEEE Netw.*, vol. 28, no. 4, pp. 46–50, Jul. 2014.

[32] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework for categorizing and applying privacy-preservation techniques in big data mining," *Computer*, vol. 49, no. 2, pp. 54–62, Feb. 2016.

[33] M. K. Kundalwal, K. Chatterjee, and A. Singh, "An improved privacy preservation technique in health-cloud," *ICT Exp.*, vol. 5, no. 3, pp. 167–172, Sep. 2019.

[34] M. Rafiei and W. M. P. van der Aalst, "Group-based privacy preservation techniques for process mining," *Data Knowl. Eng.*, vol. 134, Jul. 2021, Art. no. 101908.

[35] X. Xiao and Y. Tao, "Anatomy: Simple and effective privacy preservation," in *Proc. 32nd Int. Conf. Very Large Data Bases*, 2006, pp. 139–150.

[36] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Proc. 9th Int. Conf. Mobile Data Manag. (MDM)*, Apr. 2008, pp. 65–72.

[37] C. Saranya and G. Manikandan, "A study on normalization techniques for privacy preserving data mining," *Int. J. Eng. Technol. (IJET)*, vol. 5, no. 3, pp. 2701–2704, 2013.

[38] J. P. Near and C. Abuah, "Programming differential privacy," Univ. Vermont, Vermont, USA, Tech. Rep., 2021, vol. 1.

[39] H. Wang, S. Xie, and Y. Hong, "VideoDP: A flexible platform for video analytics with differential privacy," *Proc. Privacy Enhancing Technol.*, vol. 2020, no. 4, pp. 277–296, Oct. 2020.
[40] H. Cao, S. Liu, R. Zhao, and X. Xiong, "IFed: A novel federated learning framework for local differential privacy in power Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 5, May 2020, Art. no. 155014772091969.
[41] Y. Wang, Z. Cheng, X. Yi, Y. Kong, X. Wang, X. Xu, Y. Yan, C. Yu, S. Patel, and Y. Shi, "Modeling the trade-off of privacy preservation and activity recognition on low-resolution images," in *Proc. CHI Conf. Human Factors Comput. Syst.*, Apr. 2023, pp. 1–15.
[42] J. R. Hershey and P. A. Olsen, "Approximating the Kullback Leibler divergence between Gaussian mixture models," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2007, p. 317.
[43] H.-H. Chang, W.-Y. Chiu, H. Sun, and C.-M. Chen, "User-centric multi-objective approach to privacy preservation and energy cost minimization in smart home," *IEEE Syst. J.*, vol. 13, no. 1, pp. 1030–1041, Mar. 2019.
[44] H. Bi, J. Liu, and N. Kato, "Deep learning-based privacy preservation and data analytics for IoT enabled healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4798–4807, Jul. 2022.
[45] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Active privacy-utility trade-off against inference in time-series data sharing," *IEEE J. Sel. Areas Inf. Theory*, vol. 4, pp. 159–173, 2023.
[46] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Privacy and utility preserving sensor-data transformations," *Pervas. Mobile Comput.*, vol. 63, Mar. 2020, Art. no. 101132.
[47] H. Cao, S. Liu, L. Wu, Z. Guan, and X. Du, "Achieving differential privacy against non-intrusive load monitoring in smart grid: A fog computing approach," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 22, p. e4528, Nov. 2019.
[48] Y. Zhang, Y. Qu, L. Gao, T. H. Luan, X. Zheng, S. Chen, and Y. Xiang, "APDP: Attack-proof personalized differential privacy model for a smart home," *IEEE Access*, vol. 7, pp. 166593–166605, 2019.
[49] A. Qashlan, P. Nanda, and M. Mohanty, "Differential privacy model for blockchain based smart home architecture," *Future Gener. Comput. Syst.*, vol. 150, pp. 49–63, Jan. 2024.
[50] M. Ul Hassan, M. H. Rehmani, R. Kotagiri, J. Zhang, and J. Chen, "Differential privacy for renewable energy resources based smart metering," *J. Parallel Distrib. Comput.*, vol. 131, pp. 69–80, Sep. 2019.
[51] D. Wang, J. Ren, Z. Wang, Y. Zhang, and X. Shen, "PrivStream: A privacy-preserving inference framework on IoT streaming data at the edge," *Inf. Fusion*, vol. 80, pp. 282–294, Apr. 2022.
[52] Y. Mao, Z. Xin, Z. Li, J. Hong, Q. Yang, and S. Zhong, "Secure split learning against property inference, data reconstruction, and feature space hijacking attacks," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2023, pp. 23–43.
[53] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18.
[54] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, and D. Megías, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1418–1429, Jun. 2017.
[55] R. Dai, S. Das, S. Sharma, L. Minciullo, L. Garattoni, F. Bremond, and G. Francesca, "Toyota smarthome untrimmed: Real-world untrimmed videos for activity detection," 2020, *arXiv:2010.14982*.
[56] R. Dai, S. Das, S. Sharma, L. Minciullo, L. Garattoni, F. Bremond, and G. Francesca, "Toyota smarthome untrimmed: Real-world untrimmed videos for activity detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 2, pp. 2533–2550, Feb. 2023.
[57] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, May 2005, pp. 886–893.

SOPICHA STIRAPONGSASUTI was born in Bangkok, Thailand, in 1992. She received the B.E. degree from the Faculty of Engineering, Kasetsart University, Thailand, in 2015, and the M.E. degree from the Graduate School of Information Science, Nara Institute of Science and Technology, Japan, in 2020, where she is currently pursuing the Ph.D. degree with the Ubiquitous Computing Systems Laboratory, Graduate School of Information Science. After graduating from the university, she was an Embedded Engineer at a startup company for a year. Her research interests include pervasive computing and the IoT privacy, especially in smart home environments.

FRANCIS JEROME TIAUSAS received the B.S. degree in electronics and communications engineering from Ateneo de Manila University, Philippines, in 2011. He is currently pursuing the Ph.D. degree with the Nara Institute of Science and Technology. He has worked for several software development companies before returning to the university to pursue research in wireless sensor networks (WSNs). He is also a Researcher with the Ubiquitous Computing Systems Laboratory, Nara Institute of Science and Technology. His research interests include WSNs, privacy, and route planning algorithms.

YUGO NAKAMURA (Member, IEEE) was born in 1992. He received the B.E. degree from the Advanced Course of Production System Engineering, Hakodate College, National Institute of Technology, Japan, in 2015, and the M.E. and Ph.D. degrees from the Graduate School of Information Science, Nara Institute of Science and Technology, in 2017 and 2020, respectively. He is currently an Assistant Professor with the Graduate School, Kyushu University, where he is also with the Faculty of Information Science and Electrical Engineering. His current research interests include the Internet of Things, ubiquitous computing, and human–computer interaction. He is currently a member of ACM and IPSJ.

KEIICHI YASUMOTO (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in information and computer sciences from Osaka University, Osaka, Japan, in 1991, 1993, and 1996, respectively. He is currently a Professor with the Graduate School of Science and Technology, Nara Institute of Science and Technology. His research interests include distributed systems, mobile computing, and ubiquitous computing. He is a member of ACM, IPSJ, and IEICE.