Active Privacy-Utility Trade-off Against Inference in Time-Series Data Sharing

Ecenaz Erdemir, *Member, IEEE,* Pier Luigi Dragotti, *Fellow, IEEE,*
and Deniz Gündüz, *Fellow, IEEE*

***Abstract*— Internet of things devices have become highly popular thanks to the services they offer. However, they also raise privacy concerns since they share fine-grained time-series user data with untrusted third parties. We model the user's personal information as the *secret variable*, to be kept private from an honest-but-curious service provider, and the *useful variable*, to be disclosed for utility. We consider an active learning framework, where one out of a finite set of measurement mechanisms is chosen at each time step, each revealing some information about the underlying secret and useful variables, albeit with different statistics. The measurements are taken such that the correct value of useful variable can be detected quickly, while the confidence on the secret variable remains below a predefined level. For privacy measure, we consider both the probability of correctly detecting the secret variable value and the mutual information between the secret and released data. We formulate both problems as partially observable Markov decision processes, and numerically solve by advantage actor-critic deep reinforcement learning. We evaluate the privacy-utility trade-off of the proposed policies on both the synthetic and real-world time-series datasets.**

***Index Terms*—Inference privacy, time-series privacy, privacy funnel, active learning, actor-critic deep reinforcement learning, human activity recognition, mental workload detection.**

I. Introduction

RECENT advances in Internet of things (IoT) devices and services have increased their usage in a wide range of areas, such as health and activity monitoring, location-based services, smart speakers, and smart metering. Moreover, most service providers encourage users to share their personal data in return for a better user experience. For instance, the users can benefit from personalized dietary tips as a result of sharing their activity sensor measurements, while they can receive hotel, restaurant, or bar recommendations if they share their location. However, in most of these applications, data collected by IoT devices contain sensitive personal information about the users. The concerning fact is that as soon as the user's raw data is sent to the service provider's cloud, the sensitive information can be inferred, misused, or leaked through security vulnerabilities even if the service provider and/or the communication link are trusted third parties. For example, chronic illnesses, disabilities, daily habits, and psychological states can be revealed by health monitoring systems [1], [2], while presence at home and states of home appliances can be inferred from the collected smart meter (SM) data [3]. Hence, privacy is an important concern for the adoption of many IoT services, and there is a growing demand from consumers to keep their personal information private against malicious attackers and/or untrusted service providers (SPs), while preserving the utility obtained from these IoT services. Privacy has been widely studied in the literature [4]–[15], and a vast number of privacy measures have been introduced, including differential privacy [4], mutual information (MI) [6]–[12], total variation distance [16], maximal leakage [17], [18], and guessing leakage [19], to count a few.

The authors are with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, U.K., (e-mail: {e.erdemir17, p.dragotti, d.gunduz}@imperial.ac.uk).

This work received funding from the UKRI for the projects AIR (ERC-CoG, EP/X030806/1). For the purpose of open access, the authors have applied a Creative Commons Attribution (CCBY) license to any Author Accepted Manuscript version arising from this submission.

A. Contributions

In this paper, we consider an active learning scenario for privacy-utility trade-off (PUT) against an honest-but-curious SP in time-series data sharing. We assume that a user wants to share the "useful" part of her data with the SP. However, the SP might deduce the user's "secret" information from the shared data (e.g., location, heartbeat, temperature, energy consumption, etc.). We model the user's secret and useful data as correlated discrete random variables (r.v.'s). The user's goal is to prevent the secret from being accurately detected by the SP while revealing the useful data accurately for utility.

Differently from the existing works [6], [7], [16], [17], [19]–[21], which typically consider a time-independent data release problem, we consider a discrete-time system, where, at each point in time, the user releases a new measurement that is correlated with both the secret and the useful variables. While the objectives on the secret and the useful variables is similar to privacy preserving data mining [22]–[26], these approaches focus on sanitizing a stationary dataset while extracting the required information. On the other hand, our scenario involves transforming a time-series that becomes available to both the adversary and the user in an online fashion. We assume that the user can actively choose from among a finite number of data release mechanisms (DRMs) at each time. While each measurement reveals some information about the user's latent states, we assume that each DRM has different characteristics, i.e., conditional probability distributions. The objective is to choose a DRM at each time in an online fashion to reveal the value of the useful r.v. as quickly as possible to maximize the utility, while keeping the leakage of the sensitive information below a prescribed value.

We first consider an operational privacy measure, where the privacy of the secret r.v. is measured by the adversary's probability of correctly guessing its value. This is similar to the privacy measures in [27] and [28], but unlike those, we

are not interested in the multiplicative increase in the correct guessing probability, but its exact value. Moreover, both [27] and [28] focus on the one-shot data perturbation, whereas we are interested in a sequence of data release actions, where the leakage accumulates over time. We also consider MI between the secret r.v. and the observations as it is a popular privacy leakage metric in the literature. We note that MI-based privacy does not necessarily prevent the detection of the true secret value; instead, it limits the information leakage in an average sense [28].

Our problem is similar to time-series data privacy in the literature [8]–[11], [29]–[31], where the objective is to minimize privacy leakage by modifying the original time-series data while constraining the utility loss. However, in this work, the user selects from among multiple DRMs in an online fashion rather than modifying the non-causally available time-series data. Similar time-series data release problems are also considered in [13], [15] and [32]. However, [13] considers the PUT of a binary secret r.v. in an asymptotic regime, while [32] considers M-ary r.v.'s for an offline scenario using semi-definite programming, which has high computational complexity when fine-grained data is considered. The data release history is taken into account for M-ary r.v.'s in [15]; however, the time aspect is not considered in the PUT objective.

We consider data release policies which take the entire release history into account, and recast the problem under both privacy measures as a POMDP. After identifying the structure of the optimal policy, we use advantage actor-critic (A2C) deep reinforcement learning (DRL) to evaluate our continuous state and action probability space MDP numerically. We also use variational representations for MI estimation through neural networks.

Finally, we test the proposed policies in the human activity privacy scenario, in which we use both synthetic data and smartwatch sensor readings from *smoking activity dataset* [33]. We also test our policies for mental workload demographics privacy scenario using *Tufts fNIRS to Mental Workload (fNIRS2MW) dataset* [34], which contains brain activity recordings of adults with various demographics while performing controlled cognitive workload tasks. We compare the privacy levels achieved by the proposed policies using an SP that predicts the true values for useful data and secret from its observation history. The SP is represented by a long short-term memory (LSTM) neural network.

Our contributions can be summarized as follows:

- We pose a novel **privacy-aware active learning framework** for an online streaming of measurements. Unlike the common data perturbation or noise addition problems in the literature, where the already collected measurements are perturbed in a non-causal manner, we focus on the causal data collection mechanism. Taking into account the accumulation of data leakage over time.
- We propose a data reading/sharing policy for optimal PUT against an SP performing sequential Bayesian inference, where the privacy is measured by the confidence of the adversary in the true value of the sensitive r.v., i.e., its correct guessing probability of the secret r.v.

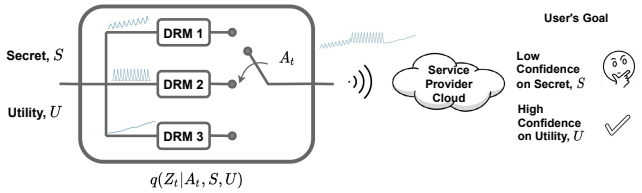


Fig. 1: System model for active PUT against the SP.

- We propose another policy based on privacy measured by the MI between the sensitive r.v. and the released data history, which minimizes the data leakage in an average sense, rather than constraining the confidence only on the true value.
- For both cases, we recast the active time-series data release problem for PUT as a POMDP, and characterize the optimal measurement mechanism when all the statistics in the system are known. We also provide a RL-based solution to evaluate both policies numerically using A2C-DRL for human activity privacy and mental workload demographics privacy datasets.

The remainder of the paper is organized as follows. We present the problem statement in Section II and the related work in Section III. Then, POMDP formulation of the problem is introduced in Section IV. MI-based privacy is introduced in Section V, and data-driven evaluation for human activity and mental workload demographics privacy are presented in Section VI-C. Finally, we conclude our work in Section VII.

II. Problem Statement

We consider a user that wants to share her data with an honest-but-curious SP in return for utility. The data reveals information about two underlying latent variables; one represents the user's sensitive information, called the *secret*, while the other is non-sensitive useful part, and is intentionally disclosed for utility. The user wants the SP to quickly detect the non-sensitive information with minimum error while keeping his confidence in the secret r.v. below a predefined level.

Fig. 1 shows an illustration of the system model with three DRMs. Let $\mathcal{S} = \{0, 1, \dots, N-1\}$ and $\mathcal{U} = \{0, 1, \dots, M-1\}$ be the finite sets of the hypotheses represented by the r.v.'s $S \in \mathcal{S}$ for the secret and $U \in \mathcal{U}$ for the non-sensitive useful information, respectively. Consider a finite set $\mathcal{A}$ of different DRMs available to the user, each modeled with a different statistical relation with the underlying hypotheses. For example, in the case of a user sharing activity data, e.g., Fitbit records, set $\mathcal{A}$ may correspond to different types of sensor measurements the user may share. Useful information the user wants to share may be the exercise type, while the sensitive information can be various daily habits. Similarly, in the case of smart meter readings, the useful information might be ON/OFF state of home appliances for smart power scheduling whereas the sensitive information might be the types of TV channels the user watches. We assume that the data revealed at time t, Z_t, is generated by an independent realization of a conditional probability distribution that depends on the true hypotheses and the chosen DRM $A_t \in \mathcal{A}$, denoted by $q(Z_t|A_t, S, U)$.

The goal is to disclose U quickly and reliably through the released data Z_t, while keeping the SP's confidence in S below a certain threshold. Let τ be the time that the SP is confident enough about the true useful variable and makes a declaration. This is also the time at which the measurements should stop since U can already be detected by the SP at the desired confidence level. The objective of the problem is to find a sequence of actions $\{A_0, \dots, A_{\tau-1}\}$, a stochastic stopping time τ and a declaration rule $d : \mathcal{A}^{\tau-1} \times \mathcal{Z}^{\tau-1} \to \mathcal{U}$ that collectively solve the following optimization problem:

$$\begin{aligned} \underset{A_0,\dots,A_{\tau-1},d}{\text{minimize}} \quad & \mathbb{E}[\tau] + \lambda P_{err}(u) \\ \text{subject to} \quad & \mathcal{C}_t(s) < L_B, \forall t \leq \tau, \forall s \in \mathcal{S}, \end{aligned} \tag{1}$$

where $P_{err}(u) = P(d(A^{\tau-1}, Z^{\tau-1}) \neq u)$ is the error probability of making wrong declaration for the true value $u \in \mathcal{U}$; $\mathcal{C}_t(s)$ is the SP's instantaneous confidence in the true sensitive value $s \in \mathcal{S}$, which is a probability distribution on s given the observation history, i.e., $P(S = s|A^{\tau-1}, Z^{\tau-1})$; L_B is a scalar of user's choice; and the expectation is taken over the action and observation distributions as well as the initial distributions of the r.v.'s. Here, by adjusting λ, we can trade-off between the speed of declaration and the SP's accuracy.

For our theoretical results, we assume that the observation statistics $q(Z_t|A_t, S, U), \forall A_t \in \mathcal{A}$, and the employed DRM A_t are known by both the user and the SP. Later, we will also consider real datasets with unknown data distributions in our simulations. To maximally confuse the SP, the user selects action A_t with a probability distribution $\pi(A_t|Z^{t-1}, A^{t-1})$ conditioned on the SP's observation history up to that time, $\{Z^{t-1}, A^{t-1}\}$. In this work, we assume that the true values of S and U are unknown to all the parties involved.

III. Related Work

Time-series data privacy has been extensively studied [8]–[11], [15], [29]–[31], [35]–[43]. Most of these works focus on the privacy relying on a single observation from a time-series, e.g., the current measurement [31], [38]–[42]. However, time-series data privacy needs to take into account more than just the individual data points since each measurement is temporally correlated throughout the entire series.

Among those that consider temporal correlations, most existing works focus on the privacy of the time-series measurements rather than hiding latent sensitive attributes [9], [10], [30], [31], [41]–[43]. In the location sharing scenario, sensitive information is the time-series data itself and the utility loss can be measured by data distortion, whereas, in many applications, the user might be interested in hiding an underlying sensitive hypothesis. For instance, the user's presence at home can be inferred from SM readings, while her daily habits can be revealed to the SP through the sensors of a wearable device. Inference privacy protects user's data from an adversary's attempt to deduce sensitive information from an underlying distribution [12], [15], [19]–[21], [44]–[46]. These techniques perform well against inference attacks, in which the adversary aims at detecting the user's underlying private information with high confidence [43]. PUT between two correlated sensitive and useful r.v.'s has also been studied under *privacy funnel* [20], which is closely related to *information bottleneck* introduced in [47]. In privacy funnel approaches [12], [19]–[21], [44]–[46], the goal is to conceal the sensitive information from SP's inference while gaining enough utility from the useful information, where both the utility and the privacy leakage are measured by MI. However, [12], [20], [21], [44] consider independent data without temporal correlations, hence, these approaches are not suitable for temporally correlated time-series data.

Differential privacy (DP), k-anonymity, information theoretic metrics and the SP's error probability are commonly used as privacy measures [8]–[11], [15], [29], [30], [35]–[43], [48]–[51]. By definition, DP prevents the SP from inferring the current data of the user, even if the SP has knowledge of all the remaining data points. K-anonymity ensures that sensitive data is indistinguishable from at least $k-1$ other data points. However, DP and k-anonymity are meant to ensure the privacy of a single point in a time-series and do not usually consider temporal correlations. As an intermediate framework between complete independence and complete correlation, *pufferfish privacy* considers low temporal correlations in time-series [46]. However, the mechanism focuses on privacy around the current data, which might ignore the inference from future and past values. There are other works that formulate privacy using the temporal correlations of infinite data streams; however, in practice, these usually follow myopic correlations with the current data, e.g., temporal correlations in a finite time window, due to the utility loss concerns raising from high noise [4], [48]–[50], [52]. For instance, the authors of [4] mention that *dependent DP* considers a Markov Quilt mechanism, which takes the correlation between certain tuples in the dataset. *Bayesian DP* in [4] provides privacy for learning iterations; however, this cannot be mapped directly to time-series data privacy since there is a different data distribution at each time step in the time-series. On the other hand, in *temporal privacy leakage* proposed in [4], only the backward privacy leakage is relevant to our method, since the future observations are not available to us in our scenario. Similarly to our proposed solution, backward privacy leakage exploits Bayesian sequential data release. However, the optimal solution in [4] can only be achieved asymptotically as time goes to infinity, while our solution is optimal in an online manner. In [48], [49] and [50], authors propose myopic approaches that consider the privacy of event sequences occurring in w successive time instances in infinite data streams. On the other hand, our scenario involves optimal stopping instead of an infinite data release, we also take the entire data history into account as opposed to a myopic w-event window.

In [42], DP in a SM with a rechargeable battery is achieved by adding noise to the meter readings before reporting to an SP. In order to guarantee DP, the perturbation must be independent of the battery state of charge. However, for a finite-capacity battery, the energy management system cannot provide the amount of noise required for preserving privacy. On the other hand, we consider a different scenario from the mentioned approaches in the sense that we cannot perturb the sensor readings as desired, e.g., we cannot simply add Gaussian or Laplacian noise, as we are limited by the inherent

stochasticity of the available measurement mechanisms. Our goal is to choose the right measurement kernel at each time instant based on the past released data.

Information-theoretic privacy (ITP) considers the statistics of the entire time-series in terms of temporal correlations, and studies privacy mechanisms that allow arbitrary stochastic transformations of data samples. Specifically, mutual information privacy focuses on the increase in one's uncertainty on the sensitive random variable in an average sense after observing a correlated measurement. DP, on the other hand, considers only a single data point privacy, and focuses on the indistinguishability between two realizations of a sensitive variable. The limited temporal correlations of standard DP is partially eliminated by group DP and pufferfish privacy, which take some degree of temporal correlations into account. However, these remain as myopic policies due to the potential loss of utility. The relation between DP and ITP is studied in the literature [53]–[55], and an upper bound on min-entropy privacy for time-series data is provided in a DP mechanism [55]. However, the other way around is not guaranteed. To reiterate, our original measure of privacy is operational based on the adversary's correct guessing probability of the secret variable. This is similar to [27] and [28], but those works are interested in the multiplicative increase in the correct guessing probability, whereas we study the PUT by considering the exact values of the adversary's correct guessing probability of both the secret and the useful r.v.'s.

Privacy metrics based on the SP's error probability focus on concealing the true realization of the sensitive information. In [13], the goal is to increase the fidelity of the shared data quantified through an additive distortion measure, while guaranteeing privacy in an online manner. Privacy leakage is measured by the error probability of the SP in detecting the distribution of the underlying data samples. In [15], the user shares her time-series data, which intrinsically contains correlated sensitive and useful information, with an untrusted SP in an online fashion. The goal is to maximize the confidence in the true useful variable for utility while keeping the confidence in the sensitive r.v. below a pre-defined level. This method is the complement of the error probability approach, and its difference from the DP and ITP is the threat model. In [15] and in this paper, the SP, which acts as an adversary, makes its final decision about the true realization of the sensitive r.v. depending on whether the maximum confidence on any realization of this variable exceeds a certain threshold. On the other hand, ITP considers the information leakage about the sensitive r.v. without considering any realization. Moreover, DP, which has been shown to have a relation to max-entropy privacy, considers the maximum indistinguishability between two realizations of the sensitive r.v., which can also be mapped to our problem as the maximum difference between the confidence on two realizations [55]. This notion of DP does not directly target keeping the confidence in any realization below a threshold, which is a part of the scenario in both [15] and this paper.

In [56], a SM system is considered assuming Markovian energy demands. Privacy is achieved by filtering the energy demand with the help of a rechargeable battery. ITP problem is formulated as an MDP, and the minimum leakage is obtained numerically through DyP, while a single-letter expression is obtained for an i.i.d. demand. This approach is extended to the scenario with a renewable energy source in [29]. In [57], PUT is examined with a rechargeable battery. Due to Markovian demand and price processes, the problem is formulated as a partially observable MDP with belief-dependent rewards (ρ-POMDP), and solved by DyP for infinite-horizon. In [11], PUT is characterized numerically by DyP for a special energy generation process.

ITP and utility for location sharing is studied in [9], and extended to generic time-series data release in [10]. The user follows a history-dependent online data release policy by minimizing the MI between the real and modified location trajectories subject to a distortion constraint. The effectiveness of the proposed approach against myopic policies and its application to GeoLife GPS trajectory dataset are presented through numerical simulations.

IV. POMDP Formulation

The above PUT can be recast as a POMDP with partially observable static states $\{S, U\} \in \mathcal{S} \times \mathcal{U}$, actions $A_t \in \mathcal{A} \cup \{d\}$, and noisy observations $Z_t \in \mathcal{Z}$. A POMDP can be reformulated as a belief-MDP with a compact yet uncountable belief state and solved using classical MDP methods. We will introduce SP's belief to determine the state variable in three steps. Firstly, we define the belief of the SP on S and U after he observes $\{Z^{t-1}, A^{t-1}\}$ by

$$\beta_t(s,u) = P(S = s, U = u | Z^{t-1} = z^{t-1}, A^{t-1} = a^{t-1}) \quad (2)$$

over the belief space $\mathbb{P}(\mathcal{B}) := \{\beta_t \in [0,1]^{M \times N} : \sum_{s \in \mathcal{S}, u \in \mathcal{U}} \beta_t(s,u) = 1\}$, where the marginal beliefs are represented by $\beta_t(u) := \sum_{s \in \mathcal{S}} \beta_t(s,u)$ and $\beta_t(s) := \sum_{u \in \mathcal{U}} \beta_t(s,u)$, respectively. The SP's confidence that $S = s$ at time t is represented by $\mathcal{C}_t(s) := \beta_t(s)$. The user's action probabilities become conditioned on the belief distribution, i.e., $\pi(A_t = a_t | \beta_t)$, while the observation probabilities are the same as before. Secondly, we introduce a new state $F_B := \{\max_{s \in \mathcal{S}} \beta_t(s) \geq L_B : \beta_t \in \mathbb{P}(\mathcal{B})\}$ for $F_B \subseteq \mathbb{P}(\mathcal{B})$, called the *forbidden-state*, which represents the condition where the constraint in (1) is violated. With slight abuse of notation, we will use F_B to denote both the forbidden state of the system and the set of belief states that fall into this state. F_B is ideally an infinite cost state; however, in practice, we assume it has a large-cost. As the third step of defining the state space, we include a terminal state to fully characterize the state in which the user stops sharing her data with the SP. We assume that after the user makes the stopping decision, the system goes to a terminal state, denoted by F_T, and remains there forever. This makes the problem an episodic MDP. Consequently, the state space becomes $\mathcal{X} = \mathbb{P}(\mathcal{B}) \cup \{F_T\}$.

We always refer to the time-independent expression of belief, i.e., β, as the current belief state. The optimal expected total cost of our problem is defined as follows:

Definition 1: For all $\beta \in \mathbb{P}(\mathcal{B})$, let the optimal value function $V^*(\beta)$ represent the optimal expected cost of problem (1), given the initial belief β. That is,

$$V^*(\beta) := \min\{\mathbb{E}[\tau] + \lambda P_{err}(u)\}, \tag{3}$$

where the minimization is with respect to τ, DRMs, and the declaration rule d.

The optimal expected total cost for active PUT against an SP can be obtained by evaluating V^* at the initial belief. This can be done by solving a DyP problem. After a single observation $\{z_t, a_t\}$, the SP updates its belief by Bayes' rule as follows:

$$\Phi(\beta_t, z_t, a_t) = \frac{q(z_t|a_t, s, u)\beta_t(s, u)}{\sum_{\tilde{s},\tilde{u}} q(z_t|a_t, \tilde{s}, \tilde{u})\beta_t(\tilde{s}, \tilde{u})}, \tag{4}$$

where the function $\Phi(\beta_t, z_t, a_t)$ represents the next belief state $\beta_{t+1}(s, u)$ in terms of the current belief, the action and the observation. We define a Markov operator $\mathbb{T}^a$ for action a, such that for any measurable function $V : \mathbb{P}(\mathcal{B}) \to \mathbb{R}$,

$$(\mathbb{T}^a V)(\beta) := \int V(\Phi(\beta, z, a)) \sum_{s,u} q(z|a, s, u)\beta(s, u)dz. \tag{5}$$

For any state $\beta \in \mathbb{P}(\mathcal{B})$, the user's data release action $a \in \mathcal{A}$ under the optimal policy results in an expected total cost of $1 + (\mathbb{T}^a V^*)(\beta)$, where time spent by the user for data release is represented by cost 1, and $(\mathbb{T}^a V^*)(\beta)$ is the expected future value of V^*. On the other hand, the user's stopping decision d results in error probability of the declaration of true useful value u with penalty λ, i.e., $\lambda P_{err}(u) := \lambda(1 - \beta(u))$. The solution for the optimal V^* is formalized by the following theorem.

Theorem 1: [58] The optimal V^* for $\beta \in \mathbb{P}(\mathcal{B})$ satisfies the fixed point equation:

$$V^*(\beta) = \min\{1 + \min_{a\in\mathcal{A}}(\mathbb{T}^a V^*)(\beta), \min_{u\in\mathcal{U}} \lambda(1 - \beta(u))\}. \tag{6}$$

Definition 2: Let a Markov stationary policy π be a stochastic kernel from the state space to the action space, including the stopping action, which determines the stopping time τ, i.e., $\mathbf{\Pi} := \mathbb{P}(\mathcal{B}) \to \mathcal{A} \cup \{d\}$. That is, the probability of choosing DRM a under policy π at state β is denoted by $\pi(a|\beta)$.

Following from Corollary 9.12.1 in [58], DyP equation (6) characterizes the optimal deterministic stationary policy π^* for $\beta \in \mathbb{P}(\mathcal{B})$. The intuition behind Theorem 1 is that the user's data release action $a^* = \arg\min_{a\in\mathcal{A}} T^a(V^*)(\beta)$ is the least costly action with cost $1 + \min_{a\in\mathcal{A}} T^a(V^*)(\beta)$, unless choosing the stopping action d and letting the SP make a decision for u is less costly, i.e., $\lambda(1 - \beta(u))$. We also ensure that for any two hypotheses $u, u' \in \mathcal{U}$, $u \neq u'$, there exists an action $a \in \mathcal{A}$, such that $D(q(z|a, s, u)||q(z|a, s, u')) > 0, \forall s \in \mathcal{S}$, where D$(\cdot||\cdot)$ denotes the Kullback-Leibler (KL) divergence. That is, hypotheses u and u' are distinguishable all the time, such that (1) has a meaningful solution.

Theorem 2: Suppose there exists a parameter $C_T > 0$, e.g., time cost, and a functional $V : \mathbb{P}(\mathcal{B}) \to \mathbb{R}_+$ such that for all belief states $\beta \in \mathbb{P}(\mathcal{B})$,

$$V(\beta) \leq \min\{C_T + \min_{a\in\mathcal{A}}(\mathbb{T}^a V^*)(\beta), \min_{u\in\mathcal{U}} \lambda C_T(1-\beta(u))\}. \tag{7}$$

Then $V^*(\beta) \geq \frac{1}{C_T} V(\beta)$ for all $\beta \in \mathbb{P}(\mathcal{B})$.

See Appendix A for the proof of Theorem 2. Theorem 2 provides a lower bound for a fixed-point expression of V^*. However, it is difficult to calculate the value of V^* and solve the DyP equation over a continuous belief space. Hence, we solve (1) numerically using an RL approach to obtain an approximate solution. Due to the belief-based privacy constraint, we call our policy *belief-privacy data release policy* (belief-PDRP), π_B. We define an instantaneous cost function for current state x and action $a \in \mathcal{A} \cup \{d\}$ as

$$c^{\pi_B}(x, a) = \begin{cases} 1, & \text{if } x = \beta \in \mathbb{P}(\mathcal{B})\backslash F_B, a \in \mathcal{A} \\ \min\limits_{u\in\mathcal{U}}(1 - \beta(u))\lambda, & \text{if } x = \beta \in \mathbb{P}(\mathcal{B})\backslash F_B, a = d \\ C_B, & \text{if } x = F_B, a \in \mathcal{A} \\ 0, & \text{if } x = F_T. \end{cases}$$

The optimal policy π_B^* is induced as a result of the minimization of $c^{\pi_B}(x, a)$. The constraint on the SP's confidence in s is enforced with a large instantaneous cost C_B for reaching state F_B, which is ideally infinite. Assuming that the system follows the optimal policy, data release actions resulting in a transition to F_B with a large-cost C_B would not be selected by the minimization problem. See the proof of Theorem 2 in Appendix A. The overall strategy for belief update is represented by the Bayes' operator as follows:

$$\Phi^{\pi_B}(x, z, a) = \begin{cases} \Phi^{\pi_B}(\beta, z, a), & \text{if } x = \beta \in \mathbb{P}(\mathcal{B}), a \in \mathcal{A} \\ F_T, & \text{if } x = \beta \in \mathbb{P}(\mathcal{B}), a = d \\ F_T, & \text{if } x = F_T. \end{cases}$$

Since the user has access to all the information that the SP has, it can perfectly track his beliefs. Hence, the user decides her own policy facilitating the SP's detection strategy, episodic behavior, and belief.

According to her strategy, the user checks whether the selected optimal action is the stopping action d. If so, she receives a cost determined by the current error probability of u with penalty λ, then transitions to the terminal state and ends the episode. If not, she checks whether the SP's belief on any secret exceeds L_B. If the user is in the *forbidden-state* she receives a large-cost C_B; otherwise, either she receives a time cost 1 or terminal state cost 0 depending on her state. If the terminal state has not already been reached and stopping action has not been taken at the moment, the user updates the SP's belief as in (4); otherwise she updates the state to the final state $x = F_T$. Using the condition (7) in Theorem 2, we write the Bellman equation induced by the optimal policy π_B^* as [59],

$$V(x) = \min_{a\in\mathcal{A}\cup\{d\}} \{c^{\pi_B}(x, a) + \mathbb{E}[V(\Phi^{\pi_B}(x, z, a))]\}, \forall x \in \mathbb{P}(\mathcal{B}). \tag{8}$$

The objective is to find a policy π_B^* that optimizes the cost function. The proposed POMDP has a continuous state space due to belief state and continuous action probabilities. Finding optimal policies for continuous state and action is PSPACE-hard [60]. In practice, to solve them by classical finite-state MDP methods, e.g., value iteration, policy iteration, and gradient-based methods, belief discretization is required [61].

While a finer discretization gets closer to the optimal solution, it expands the state space; hence, the problem complexity. Hence, we use A2C-DRL to numerically solve the continuous state and action space MDP in Section VI-C.

In the next section, we consider a MI-based privacy policy, which measures the privacy leakage by MI and preserves the privacy in an average sense.

V. MI as Privacy Constraint

In this section, we consider a scenario, in which the user is interested in limiting the information leakage about the sensitive information in an average sense, rather than hiding its true value. For instance, the SP might be confused about the true secret; however, he might still have an idea about which secret values are unlikely. More concretely, consider a secret r.v. with alphabet size of three, e.g., $\mathcal{U}=\{1,2,3\}$. From the perspective of confidence, the belief of $\beta(U=1)=1/2$, $\beta(U=2)=1/4$, $\beta(U=3)=1/4$ would be the same as $\beta(U=1)=1/2$, $\beta(U=2)=1/2$, $\beta(U=3)=0$, while the latter clearly has additional information about the secret resulting in reduced uncertainty. To quantify the reduction in uncertainty, we refer to the definition of MI which measures the amount of information that two random variables share. In other words, it quantifies the degree to which the values of one variable can help predict, or reduce the uncertainty of, the values of the other variable. MI between two random variables X and Y can be calculated by $I(X;Y)=\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P(x,y)\log\left(\frac{P(x,y)}{P(x)P(y)}\right)$. Therefore, we measure the privacy loss by the MI between the secret variable S and the observation history $\{Z^t,A^t\}$ for $t\leq\tau$. According to her policy, the user wants to minimize the error on useful information as quickly as possible while keeping the total MI between the secret and the observations below a prescribed level, i.e., $\forall Z\in\mathcal{Z}$ and $\forall A\in\mathcal{A}$,

$$\begin{aligned} &\text{minimize} && \mathbb{E}[\tau]+\lambda P_{err}(u) \\ &\text{s.t.} && I(S;Z^t,A^t)<L_{MI}, \quad \forall t\leq\tau,\forall S\in\mathcal{S} \end{aligned} \tag{9}$$

where L_{MI} is a scalar of the user's choice.

MI is commonly used both as a privacy and a utility measure in the literature [8], [10], [20]. Here, it is used as a privacy measure to control PUT between the useful variable and the secret. Due to the MI-based privacy constraint in (9), we call this policy *MI-privacy data release policy* (MI-PDRP), π_{MI}. MI between S and (Z^T,A^T) over time T is given by

$$I(S;Z^T,A^T)=\sum_{t=1}^{T} I(S;Z_t,A_t|Z^{t-1},A^{t-1}). \tag{10}$$

Theorem 3: The instantaneous MI cost between the secret and the observations induced by policy π_{MI} at time t can be written as:

$$\begin{aligned} I^{\pi_{MI}}(S;Z_t,A_t|\beta) = &-\sum_{s,u,z_t,a_t} q(z_t|a_t,s,u)\pi(a_t|\beta)\beta(s,u) \\ &\times\log\frac{\sum_{\tilde{u}} q(z_t|a_t,s,\tilde{u})\pi(a_t|\beta)\beta(s,\tilde{u})}{\beta(s)\sum_{\bar{s},\bar{u}} q(z_t|a_t,\bar{s},\bar{u})\pi(a_t|\beta)\beta(\bar{s},\bar{u})}. \end{aligned} \tag{11}$$

See Appendix B for the proof.

As before, we define the state in three stages, i.e., the belief, the *forbidden-MI-state* as $F_{MI}:=\{\beta_t(s): I^{\pi_{MI}}(S;Z^t,A^t)\geq L_{MI},\forall t\leq\tau\}$ for $F_{MI}\subseteq\mathbb{P}(\mathcal{B})$, where the constraint in (9) is violated, and the final state F_T in which the episode terminates. As before, we will use F_{MI} to denote both the forbidden state and the set of forbidden states for convenience. We define an instantaneous cost function, $c^{\pi_{MI}}(x,a)$, for current state $x\in\mathcal{X}=\mathbb{P}(\mathcal{B})\cup\{F_T\}$ and action $a\in\mathcal{A}\cup\{d\}$, which induces the optimal MI-PDRP π^*_{MI} when minimized:

$$c^{\pi_{MI}}(x,a)=\begin{cases} 1, & \text{if } x=\beta\in\mathbb{P}(\mathcal{B})\backslash F_{MI}, a\in\mathcal{A} \\ \min\limits_{u\in\mathcal{U}}(1-\beta(u))\lambda, & \text{if } x=\beta\in\mathbb{P}(\mathcal{B})\backslash F_{MI}, a=d \\ C_{MI}, & \text{if } x=F_{MI}, a\in\mathcal{A} \\ 0, & \text{if } x=F_T. \end{cases}$$

The constraint on the total MI leakage from S is enforced with a large-cost C_{MI} for state F_{MI}. Assuming that the system follows the optimal MI-PDRP π^*_{MI}, F_{MI} would not be visited at all. The overall strategy for belief update is represented by the Bayes' operator as follows:

$$\Phi^{\pi_{MI}}(x,z,a)=\begin{cases} \Phi^{\pi_{MI}}(\beta,z,a), & \text{if } x=\beta\in\mathbb{P}(\mathcal{B}), a\in\mathcal{A}, \\ F_T, & \text{if } x=\beta\in\mathbb{P}(\mathcal{B}), a=d, \\ F_{MI}, & \text{if } x=\beta(s,u)\in\mathbb{P}(\mathcal{B}) \\ & \sum\limits_{i=1}^{t} I^{\pi}(S;Z_i,A_i|\beta_i)\geq L_{MI}, \\ F_T, & \text{if } x=F_T. \end{cases}$$

Theorem 2 holds for (9) when we replace $\{c^{\pi_B},\Phi^{\pi_B},F_B\}$ with $\{c^{\pi_{MI}},\Phi^{\pi_{MI}},F_{MI}\}$, and provides a lower bound for the value function V^* for all $\beta\in\mathbb{P}(\mathcal{B})$. Hence, to find the policy π^*_{MI}, we solve the Bellman equation (8) using RL for c^{π_B} and Φ^{π_B}. This policy minimizes the SP's error on the true value of u in the quickest way while constraining the MI leakage from not only true secret s but all possible values for S.

A. Estimating MI

The exact computation of MI is possible when the data distribution is known. However, in most practical scenarios, the user's data distribution is not known or it is inaccurate. Hence, we approximate $I(S;Z^T,A^T)$ via a variational representation which is inspired by Barber-Agakov MI estimation for single letter MI [62]. Since (10) is history-dependent, we modify this variational bound to a history dependent expression as follows:

$$I(S;Z_t,A_t|Z^{t-1},A^{t-1}) \tag{12}$$

$$= H(S|Z^{t-1},A^{t-1})-H(S|Z^t,A^t) \tag{13}$$

$$= H(S|Z^{t-1},A^{t-1})+\mathrm{D}(P(S|Z^t,A^t)||Q(S|Z^t,A^t)) + \mathbb{E}[\log Q(S|Z^t,A^t)] \tag{14}$$

$$= H(S|Z^{t-1},A^{t-1})+\max_{Q(S|Z^t,A^t)}\mathbb{E}[\log Q(S|Z^t,A^t)] \tag{15}$$

where (13) follows from the definition of MI, (14) holds for any distribution $Q(S|Z^t,A^t)$ over $\mathcal{S}$ given the values in $\mathcal{Z}^t\times\mathcal{A}^t$, which represents what the belief would be

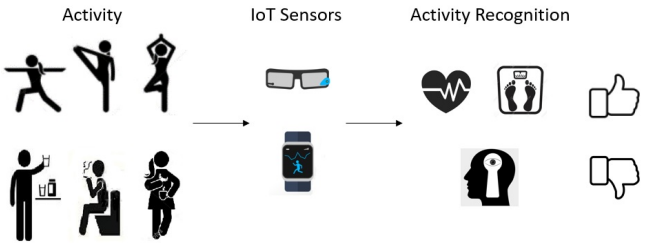


Fig. 2: Activity recognition with wearable IoT devices does not only infer physical exercise but also sensitive daily habits.

after observing (A_t, Z_t), and (15) follows from the fact that maximum is attained when $Q(S|Z^t, A^t) = P(S|Z^t, A^t)$.

Given $(Z^{t-1}, A^{t-1}) = (z^{t-1}, a^{t-1})$, we can rewrite the variational representation for the MI conditioned on the neural estimation of the current belief $\hat{\beta}(S) = Q(S|Z^{t-1}, A^{t-1})$ as

$$I(S; Z_t, A_t|\hat{\beta}) = H(\hat{\beta}(S)) + \max_{Q(S|Z_t, A_t, \hat{\beta})} \mathbb{E}[\log Q(S|Z_t, A_t, \hat{\beta})], \tag{16}$$

where $H(\hat{\beta}(S)) = -\sum_{s\in\mathcal{S}} \hat{\beta}(s) \log \hat{\beta}(s)$, and the expectation is with respect to $(S, Z_t, A_t) \sim \hat{\beta}(S), \pi(A_t|\hat{\beta}), q(Z_t|A_t, S, U)$. Since the current belief realization is known to both the user and the SP, $H(\hat{\beta}(S))$ is a constant. Numerical estimation of the MI via neural networks is explained in Section VI-C2.

VI. Numerical Results

In this section, we present our results for both synthetic data, human activity privacy and mental workload demographics privacy use-cases. In the synthetic data case, we assume that all the distributions of the DRM are known by both the user and the SP, while the other two cases employ the distributions that are learned from real datasets. In the human activity privacy use-case, we focus on the sensors in wearable devices as an example of DRMs, and their measurements as time-series data. In this scenario, the user shares sensor readings of her wearable device with the SP, while performing physical activities, with the goal of tracking the type and duration of her activities. However, as in Fig. 2, not only useful activities, such as exercise type, but also sensitive activities, such as smoking, drinking, or eating habits, can be inferred from these readings, which the user may not want to share with the SP as the SP can exploit such information for a commercial benefit at the detriment of the user. Hence, the user shares a single sensor reading from among multiple sensors at a time such that the useful activity is revealed to the SP while his confidence in the sensitive activity is kept hidden at a pre-defined level.

In the mental workload demographics privacy use-case, we treat fNIRS sensors as the DRMs that release brain activity measurements in the form of a multivariate time-series. The users from various racial backgrounds labeled as *white*, *asian* and *other*, share their brain activities for a mental workload classification experiment while performing memory intensive tasks. Even though the main task is to classify the mental workload intensity level as $U = \{0, 1, 2, 3\}$, sensitive information about the user's demographics can also be inferred during the experiment. Therefore, the user shares a single sensor reading at a time to reveal the mental workload while keeping the demographics hidden.

The POMDP formulation in Section IV enable us to numerically approximate the proposed policies using RL. In RL, an agent discovers the best action to take in a particular state by receiving instant rewards or costs from the environment [63]. POMDPs with continuous belief and action spaces are difficult to solve numerically by using classical MDP solution methods. Actor-critic RL algorithms combine the advantages of value-based (critic-only) and policy-based (actor-only) methods, such as low variance and continuous action probability producing capability. Therefore, we use A2C-DRL for the numerical evaluation of our problem.

A. A2C-DRL

In the A2C-DRL algorithm, the actor represents the policy structure and the critic estimates the value function [63]. In our setting, we parameterize the value function by the parameter vector $\theta \in \Theta$ as $V_\theta(x)$, and the stochastic policy by $\xi \in \Xi$ as $\pi_{\boldsymbol{\xi}}$. The error between the critic's estimate and the target differing by one-step in time is called temporal difference (TD) error [64]. The TD error for the experience tuple $(x_t, \pi(a_t|x_t), z_t, x_{t+1}, c_t(x_t, a_t))$ is estimated as:

$$\delta_t = c_t(x_t) + \gamma V_{\theta_t}(x_{t+1}) - V_{\theta_t}(x_t), \tag{17}$$

where $c_t(x_t) + \gamma V_{\theta_t}(x_{t+1})$ is called the TD target, and γ is a discount factor chosen close to 1 to approximate the Bellman equation for our episodic MDP. Instead of using the value functions in actor and critic updates, we use the advantage function to reduce the variance from the policy gradient. The advantage is approximated by TD error. Hence, the critic is updated by gradient ascent as:

$$\theta_{t+1} = \theta_t + \eta_t^c \nabla_\theta \ell_c(\theta_t), \tag{18}$$

where $\ell_c(\theta_t) = \delta_t^2$ is the critic loss, and η_t^c is the learning rate of the critic at time t. The actor is updated similarly as:

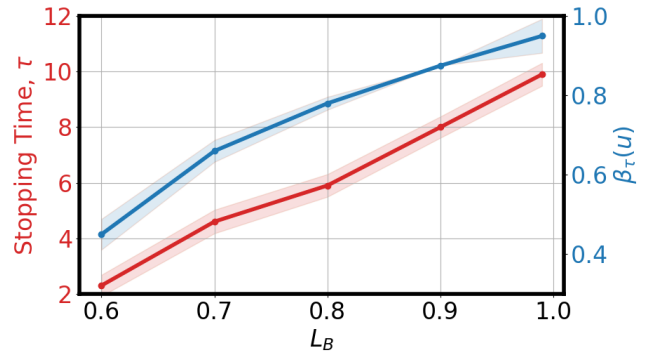
$$\xi_{t+1} = \xi_t - \eta_t^a \nabla_\xi \ell_a(\xi_t), \tag{19}$$

where $\ell_a(\xi_t) = -\ln(\pi(a_t|x_t, \xi_t))\delta_t$ is the actor loss and η_t^a is the actor's learning rate. In the implementation, we represent the actor and critic by fully connected deep neural networks (DNNs) with two hidden layers of 256 nodes and *Leaky-ReLU* activation. The critic DNN takes the current state x of size $N \times M$ as input and outputs the corresponding state value for the current action probabilities $V_\theta^\xi(x)$. The actor takes the state as input, and outputs the corresponding action probabilities $\{\xi^0, \ldots, \xi^{|\mathcal{A}|}\}$ from a *softmax* layer for $a \in \mathcal{A} \cup d$.

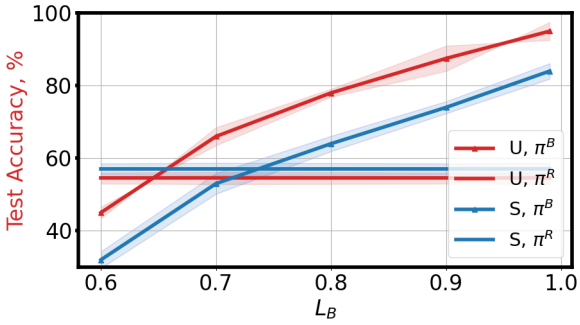
B. Synthetic Data Use-Case

The synthetic data scenario represents the situations where the probability distributions of DRMs and belief update rules are known by both the user and the SP, while only the actions are learned by the privacy mechanism.

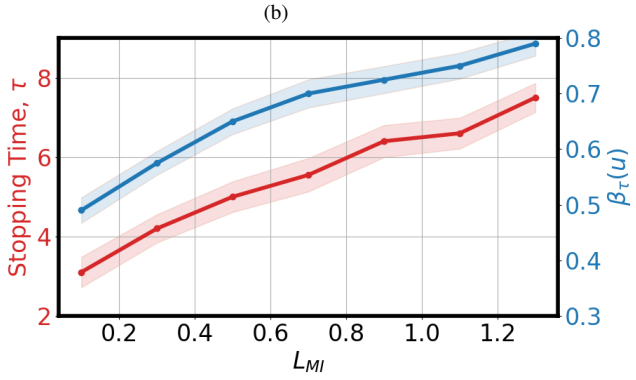
We create a dataset for $|\mathcal{A} \cup \{d\}|$=4, $|\mathcal{S}|$=3, $|\mathcal{U}|$=3, $|\mathcal{Z}|$=50 and uniformly distributed S and U, and $L_B \in$



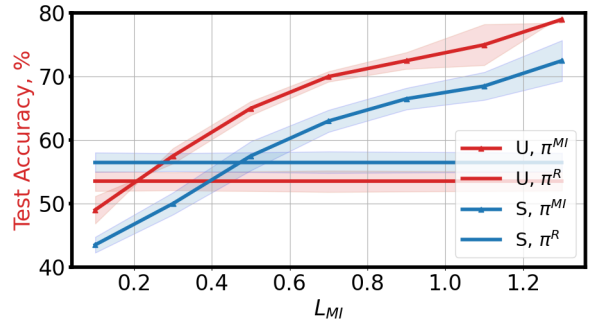
(a)



(b)



(c)



(d)

Fig. 3: Belief-PDRP's, π_B, (a) stopping time τ and $\beta(u)$, and (b) SP's accuracy for the secret and the useful information with respect to L_B, and MI-PDRP's, π_{MI}, (c) stopping time τ and $\beta(u)$, and (d) SP's accuracy for the secret and the useful information with respect to L_{MI}.

TABLE I
SELECTED ACTIVITIES AND SMARTWATCH SENSORS FROM SMOKING ACTIVITY DATASET.

Sensors:	**A**	**Activities:**	**(S,U)**
Accelerometer	0	Sitting	(0,0)
Gyroscope	1	Standing	(0,1)
Magnetometer	2	Walking	(0,2)
Linear-accelerometer	3	Sitting while smoking	(1,0)
		Standing while smoking	(1,1)
		Walking while smoking	(1,2)
		Sitting while drinking	(2,0)
		Standing while drinking	(2,1)

$\{0.6, 0.7, 0.8, 0.9, 0.99\}$. Observation probabilities are selected such that each action distinguishes a different pair of hypotheses well for both S and U. For example, we create a matrix with each row representing the conditional distribution of z for different (a, s, u) realizations. For sensor a=0, we use $\mathcal{N}(0, \sigma_j)$ for (s, u)=$\{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$, $\mathcal{N}(1, \sigma_j)$ for $(s, u) = (2, 0)$, $\mathcal{N}(2, \sigma_j)$ for $(s, u) = (2, 1)$, and $\mathcal{N}(3, \sigma_j)$ for $(s, u) = (2, 2)$, and we normalize through the columns representing z. Here, σ_j's are chosen randomly from the interval $[0.5, 1.5]$ for each (a, s, u) with index j=$\{1, .., N \times M \times |\mathcal{A}|\}$. This sensor discloses s=2 case more than the other secrets. Moreover, a=1 and a=2 reveal more information for s=1 and s=0 cases, respectively.

Fig. 3a shows the average stopping time τ and the maximum belief on u, $\beta(u)$, with respect to L_B for the belief-PDRP, π_B. As the constraint on $\beta(s)$ is relaxed, the stopping time increases as well as the maximum $\beta(u)$. In Fig. 3b, on the other hand, we present the prediction accuracy of the true-useful activity u from the belief calculation. Red lines in Fig. 3b represent accuracy on u, and blue lines show the accuracy on s. The gap between the accuracy shows the effectiveness of the proposed policy π_B in minimizing the SP's error probability of u in the quickest way while keeping his confidence in s below the threshold for the synthetic data.

Fig. 3c shows the average stopping time τ and the maximum confidence in u, $\hat{\beta}(u)$, with respect to L_{MI} for the MI-PDRP, π_{MI}. As before, when the constraint on MI is relaxed, the stopping time increases as well as the maximum $\hat{\beta}(u)$. In Fig. 3d, red lines represent accuracy on u, and blue lines show the accuracy on s. The comparisons for both policies reveal that randomly shuffling the DRMs results in a similar level of accuracy for both variables. However, the proposed policies exhibit a significant increase in the accuracy gap between the useful and secret variables. This enhancement allows for the decision-making process to be performed on the U while maintaining a low accuracy for S. When we compare the two policies we propose, despite the similar accuracy results for both π_{MI} and π_B, π_B seems more effective in hiding the true realization of S. This is because MI-PDRP provides PUT by constraining the statistics of all the realizations of S rather than only the true realization.

C. Human Activity Privacy Use-Case

In the human activity privacy scenario, we use *smoking activity dataset* [33] which contains more than 40 hours of sensor measurements for activities, such as smoking while walking, drinking while standing, sitting, etc. We use measurements

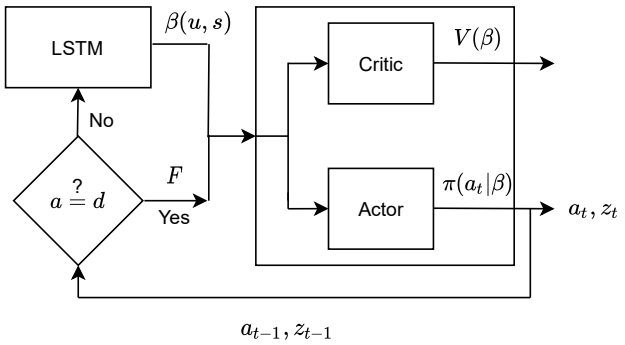


Fig. 4: A2C-DRL process for belief-PDRP, π_B.

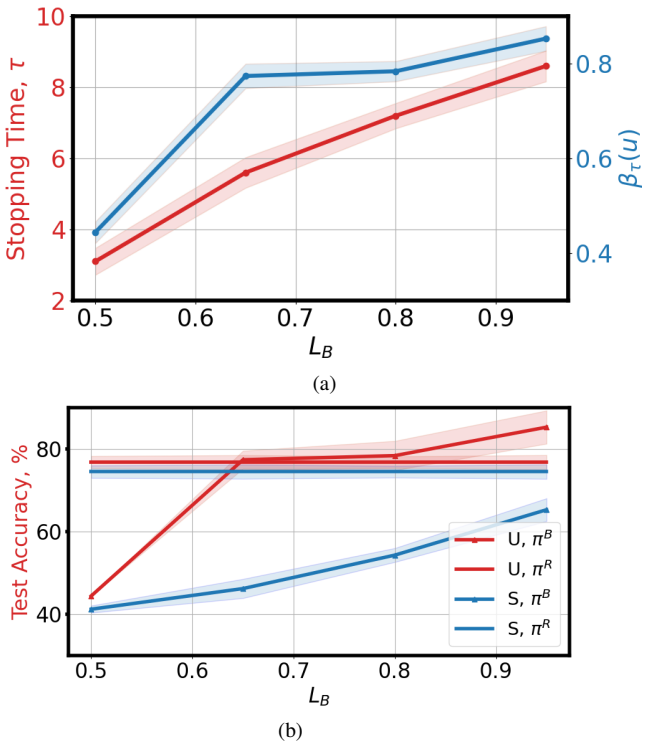


Fig. 5: (a) Stopping time τ and $\hat{\beta}(u)$, and (b) SP's accuracy for the secret and the useful information with respect to L_B.

from four selected sensors of a smartwatch, i.e., $|\mathcal{A}\cup\{d\}| = 5$. Table I shows these sensors and sensitive-useful activity pairs from the dataset. We learn the probability distributions together with the actions from real-world measurements.

1) Numerical Results for Belief-PDRP, π_B: In this section, we evaluate the PUT of the proposed optimal policy π_B for the smoking activity dataset. We model the SP by a long short-term memory (LSTM) recurrent neural network with parameters ϕ, which predicts the true useful variable u and secret s. The LSTM-based predictor has 2 layers with 128 nodes and 2 look-backs, and inputs the past observations $\{z^{t-1}, a^{t-1}\}$. The output is a probability distribution representing the belief vector $\hat{\beta}_\phi(S,U)$ obtained by minimizing a cross-entropy loss between $\hat{\beta}_\phi(S,U)$ and true values of $\{S,U\}$. This is equivalent to maximizing the log-likelihood of $\hat{\beta}_\phi(S,U)$, i.e.,

$$H(\beta,\hat{\beta}) = -\sum_{s,u}\beta(s,u)\log(\hat{\beta}(s,u)) = -\mathbb{E}_{s,u}[\log(\hat{\beta}(s,u))].$$

To train the LSTM SP beforehand, we split the training data into 3 portions. One is for pre-training the LSTM SP, which will be used during A2C-DRL, one is for online A2C-DRL training, and the last portion is to train an SP, i.e., LSTM predictor, for testing the performance of PUT with A2C-DRL. Let π_R be a random policy with uniform action probabilities. We create observation pairs $\{Z_t, A_t\}$ for LSTM training by randomly sampling actions A_t from π_R, and obtaining time-series Z_t from the corresponding portion of the dataset. We also used $C_T = 0.5$ for the time cost, and $\lambda = 50$.

Fig. 4 shows the A2C-DRL process in which LSTM is used as an online state predictor from the past observations. The user checks if the termination action, i.e., $a_{t-1} = d$, has been taken, then she accordingly terminates the process. Otherwise, she predicts the current belief with the LSTM network and selects an action a_t via the actor. The actor-critic network updates its parameters with the state value $V(\beta)$ and action probability $\pi(a_t|\beta)$ accordingly. Sensor reading z_t is observed as per the selected action, and the observation pair z_t, a_t is shared with the SP.

Fig. 5a shows the average stopping time τ and the predicted maximum belief on u, $\hat{\beta}(u)$, with respect to L_B for the belief-PDRP, π_B. As the constraint on $\hat{\beta}(s)$ is relaxed, the stopping time increases as well as the maximum $\hat{\beta}(u)$. In Fig. 5b, on the other hand, no-PUT and PUT cases are compared in terms of prediction accuracy of the test SP on true-useful activity u and the secret s, where the accuracy of the SP for the randomly generated A_t and corresponding Z_t represents the no-PUT case, while its accuracy for the A2C-DRL generated actions A_t and Z_t represents the PUT case. Red lines in Fig. 5b represent accuracy on u, and blue lines show the accuracy on s. The flat lines show the no-PUT case which does not depend on L_B, and the curved lines represent the PUT case. While the gap between the accuracy of u and s is very low for random policy (no-PUT case), it is very large for π_B (PUT case). This shows the effectiveness of the proposed policy π_B in minimizing the SP's error probability of u in the quickest way while keeping his confidence in s below the threshold. On the other hand, generating random actions from a random policy does not yield a sophisticated strategy to reveal u and hide s. The largest gap, i.e., the best performance of π_B, occurs at $L_B = 0.65$ for π_B.

2) Numerical Results for MI-PDRP, π_{MI}: In this section, we model the SP using two components; one is an LSTM-based belief predictor with 2 layers of 128 nodes and 2 look-backs, and the other one is a feed-forward neural network (FFNN)-based observation generator with 3 layers of 256 nodes, where the output determines the mean μ and standard deviation σ of a Gaussian distribution. As before, we use $C_T = 0.5$ for the time cost, and $\lambda = 50$.

As in Section VI-C1, we train the LSTM network with parameters ϕ by minimizing a cross-entropy loss between the observations $\{Z^{t-1}, A^{t-1}\}$ and $\{S,U\}$, which is equivalent to maximizing the log-likelihood of $\hat{\beta}_\phi(S,U)$. As a result, KL divergence between the real belief distribution β and the

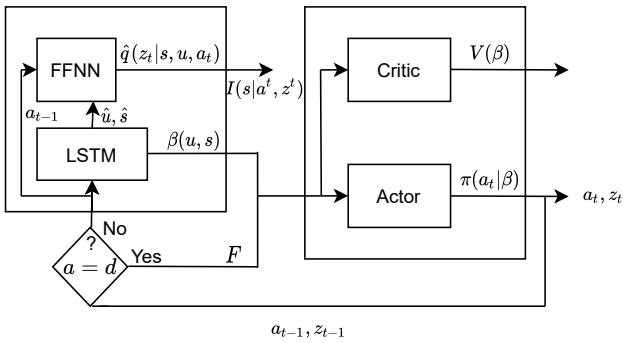


Fig. 6: A2C-DRL process for MI-PDRP, π_{MI}.

predicted distribution $\hat{\beta}_\phi$ goes to zero when the log-likelihood is maximized [62]. In addition, we estimate $q(Z_t|A_t,S,U)$, which is represented by a Gaussian distribution,

$$\hat{q}(Z_t|A_t,S,U)=\mathcal{N}(Z_t|(\mu,\Sigma))=f_\psi(A_t,S,U), \quad (20)$$

where (μ,σ) are determined by a FFNN f_ψ by maximizing its log-likelihood. During A2C-DRL, we sample observations Z_t and A_t to calculate the variational bound for MI using the pre-trained FFNN and LSTM networks which satisfy the maximization in (16). We approximate the MI by sampling k observations $\{z_t^i,a_t^i\}_i^k\sim\hat{q}(z_t|a_t,\hat{s},\hat{u}),\pi_{MI}(a_t|\hat{\beta})$, and using the predictions for the next k belief states $\{Q(s|z_t^i,a_t^i,\hat{\beta})\}_i^k$ as follows:

$$\hat{I}(S;Z_t,A_t|\phi,\psi) = H(\hat{\beta}_\phi)+\frac{1}{n}\sum_{j=1}^{n}\Big[\frac{1}{k}\sum_{i=1}^{k}\log[Q_\psi((\hat{s}^j|z_t^i,a_t^i,\hat{\beta}_\phi))]\Big], \quad (21)$$

where $\hat{s}^j$ is a realization of s sampled from the predicted belief vector $\hat{\beta}_\phi(s)$. Fig. 6 illustrates the A2C-DRL process with belief and MI calculation using pre-trained LSTM and FFNN. The user checks if the termination action, i.e., $a_{t-1}=d$, has been taken. If so, she accordingly terminates the process. Otherwise, she predicts the current belief from the previous observations using the LSTM network and takes action a_t. The actor-critic network updates its parameters with the state value $V(\beta)$ and action probability $\pi(a_t|\beta)$ accordingly. Sensor measurement is observed as per the selected action, and the observation pair z_t,a_t is shared with the SP. $\hat{I}(\hat{S}|A^t,Z^t|\beta_t)$ is calculated by the SP using previous action a_{t-1} and $(\hat{s},\hat{u})$ according to (21).

Fig. 7a shows the average stopping time τ and the maximum confidence in u, $\hat{\beta}(u)$, with respect to L_{MI} for the MI-PDRP, π_{MI}. As the constraint on MI is relaxed, the stopping time increases as well as the maximum $\hat{\beta}(u)$. In Fig. 7b, activity prediction accuracy of the test SP for observations (Z_t,A_t) generated by random policy π_R and π_{MI} are compared. Red lines in Fig. 7 represent accuracy on u, and blue lines show the accuracy on s. Similarly to Section VI-C1, the gap between the accuracy of u and s is very low for random policy, while it is large for π_{MI}. This shows that the proposed policy π_{MI} minimizes the SP's error probability of u in a speedy manner while keeping the information leakage from s below

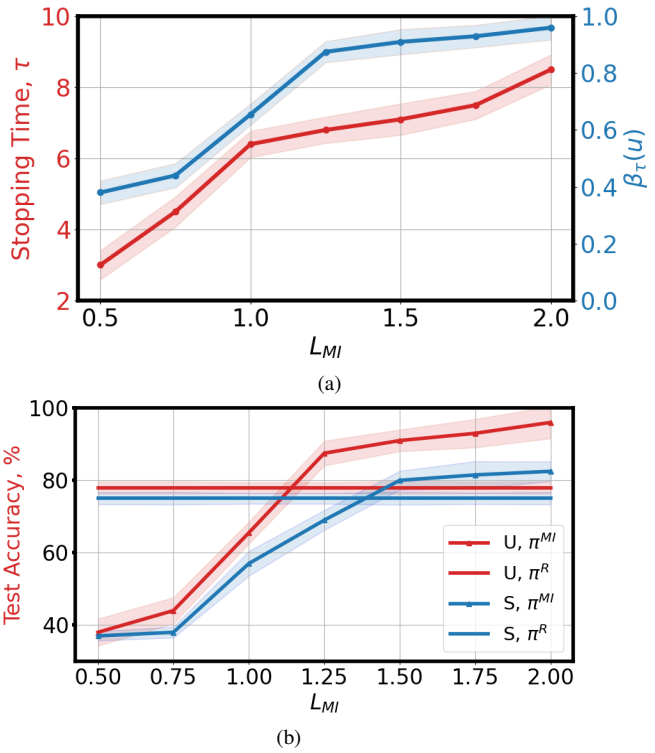


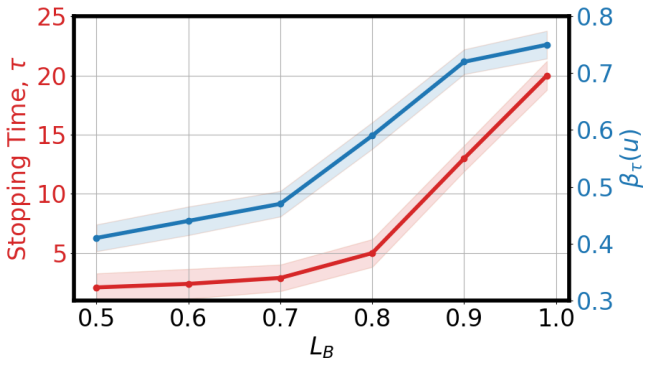
Fig. 7: (a) Stopping time τ and $\hat{\beta}(u)$ and (c) SP's accuracy for the secret and the useful information with respect to L_{MI}.

the threshold. Although π_{MI} shows similar results with π_B, π_B is more effective in hiding the true realization of S. This is because MI-PDRP provides PUT by constraining the statistics of all the realizations of S rather than only the true realization. The largest gap in Fig 7, i.e., the best performance of π_{MI}, occurs at $L_{MI}=1.2$ for π_{MI}.

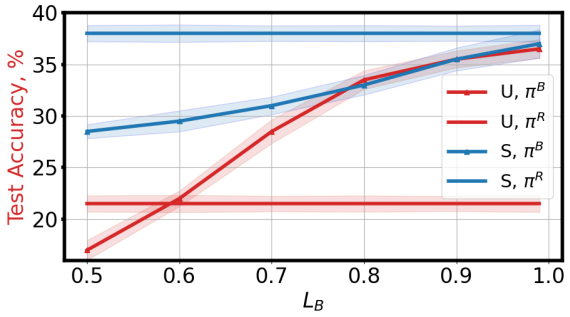
D. Mental Workload Demographics Privacy Use-Case

Herein, we consider a cognitive workload classification scenario in which we focus on preserving the privacy of subject demographics. We use the fNIRS2MW dataset [34] that contains brain activity recordings from 68 participants while they are performing certain memory tasks. The dataset is labeled according to the working memory intensity levels as $U=\{0,1,2,3\}$. We group 8-ary multivariate time-series sensor measurements into 4 DRMs of size 2, i.e., $|\mathcal{A}\cup\{d\}|=5$. For each action realization, we collect 4 samples of observations. Moreover, the secret r.v. is selected as the ethnic background of the subjects, namely $S=\{White,Asian,Other\}$. We create a time-series from the sensor readings by randomly choosing subject data from various ethnicities. As before, we learn the probability distributions as well as the actions from real-data.

1) Numerical Results for Belief-PDRP, π_B: In this section, we evaluate the PUT of π_B for the mental fNIRS2MW dataset. We use the same SP architecture and A2C-DRL process as introduced in the human activity privacy use-case. We split the fNIRS2MW dataset into 3 parts for (1) pre-training the SP network for A2C-DRL training, (2) A2C-DRL online training, and (3) pre-training the SP network for A2C-DRL testing. As

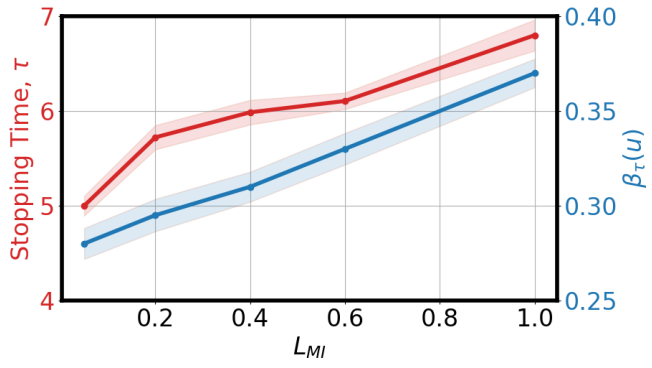


(a)

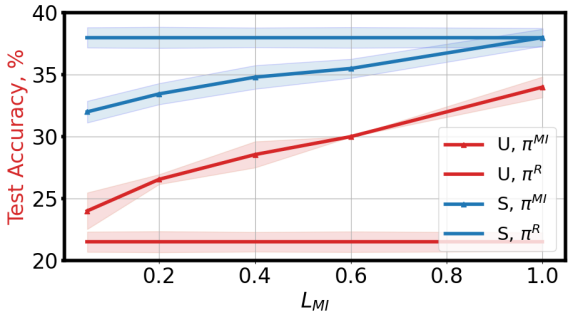


(b)

Fig. 8: (a) Stopping time τ and $\hat{\beta}(u)$ and (c) SP's accuracy for the secret and the useful information with respect to L_B.



(a)



(b)

Fig. 9: (a) Stopping time τ and $\hat{\beta}(u)$ and (c) SP's accuracy for the secret and the useful information with respect to L_{MI}.

before, π_R represents the random policy with uniform action probabilities. We set $C_T = 0.5$ for the time cost, and $\lambda = 50$.

Fig. 8a shows τ and the maximum $\hat{\beta}(u)$ with respect to L_B for the policy π_B in the demographics privacy use-case. As we relax the belief constraint, the stopping time and the maximum $\hat{\beta}(u)$ increase simultaneously. Compared to the activity privacy use-case, here, we observe lower confidence in the useful variable for longer stopping time and larger privacy constraints. This is due to the statistics of the dataset which reveals relatively less information about the hypotheses for detection tasks than the previous use-case. Fig. 8b shows a comparison between no-PUT and PUT cases in terms of the SP accuracy on u and s. Red lines represent the SP accuracy on u, and blue lines show the accuracy on s. In Fig. 8b, we observe that π_B (PUT case) effectively reduces the accuracy in s and increases the accuracy in u, compared to the baseline policy. This result is aligned with the previous use-case and shows that the policy π_B provides PUT evidently.

2) Numerical Results for MI-PDRP, π_{MI}: Here, we repeat the process described in Section VI-C2 using the same architectures and parameters for fNIRS2MW dataset. Fig. 9a shows the average τ and $\hat{\beta_\tau u}$ performance of the MI-PDRP policy with respect to the privacy constraint for demographics privacy use-case. Compared to the previous use-case, here, π_{MI} achieves lower SP confidence in u for the same level of information leakage in a longer stopping time. As mentioned earlier, this is due to the dataset statistics. The PUT gained by the policy π_{MI} in comparison with the no-PUT case, i.e., π_R, is shown in the Fig. 9b. As expected, π_{MI} reduces the accuracy in s while increasing the accuracy in u compared to the no-PUT case. We also observe that π_{MI} policy achieves the same level of accuracy reduction in s as π_B, while the gain in the accuracy in u is less than that of π_B.

VII. Conclusion

We studied the PUT in time-series data release to a SP. The goal of the user is to reveal the true value of a latent utility variable while keeping the secret variable private from the SP. In a sense, the SP is the legitimate receiver for the utility variable, while acting as the adversary for the sensitive variable. In particular, we measured the utility by the confidence of the SP in the latent useful information. For privacy, we considered both the confidence of the SP on the sensitive information and the MI between the sensitive variable and the revealed measurements. We proposed active sequential data release policies to minimize the error probability on the true useful variable in a speedy manner while constraining the confidence of the SP or the MI leakage for the secret variable. We provided a POMDP formulation of the problem and used A2C-DRL for numerical evaluations. Utilizing DNNs, we numerically evaluated the PUT curve of the proposed policies for *smoking activity* and *fNIRS2MW* datasets. While in the former useful and sensitive activities are revealed to the SP through smartwatch sensors selected by the user, in the latter, the user's mental workload intensity levels that also contain their demographics are revealed through the brain activity measurements. We examined the effectiveness of the optimal belief-PDRP and MI-PDRP schemes using an LSTM-based adversary network. According to the numerical results, we have seen that the proposed data release policies provide

a significant privacy advantage compared to random sensor selection. We have also seen that constraining the MI does not necessarily hide the true value of the secret at the same level as the belief-PDRP. However, this approach may be more useful when the objective is not necessarily to hide the true value of the secret but limit the knowledge of the SP in an average sense. We have also shown that decision time gets longer when the constraint on the secret is relaxed.

REFERENCES

[1] R. Shanthapriya and V. Vaithianathan, "Ecg-based secure healthcare monitoring system in body area networks," in *2018 Fourth Int'l Conf. on Biosignals, Images and Instrum. (ICBSII)*, March 2018, pp. 206–212.

[2] T. Wearing and N. Dragoni, "Security and privacy issues in health monitoring systems: ecare@home case study," in *Proc. of the Int'l Conf. on IoT Technol. for HealthCare*, 10 2016, pp. 165–170.

[3] G. Giaconi, D. Gündüz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *IEEE Signal Processing Magazine*, vol. 35, no. 6, pp. 59–78, Nov 2018.

[4] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, "Quantifying differential privacy under temporal correlations," in *2017 IEEE 33rd Int'l Conf. Data Eng. (ICDE)*, April 2017, pp. 821–832.

[5] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-aware communication over a wiretap channel with generative networks," *ArXiv*, vol. abs/2110.04094, 2021.

[6] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 1401–1408.

[7] A. Zamani, T. Oechtering, and M. Skoglund, "A design framework for epsilon-private data disclosure," *ArXiv*, vol. abs/2009.01704, 2020.

[8] E. Erdemir, D. Gündüz, and P. L. Dragotti, "Smart meter privacy," in *Privacy in Dynamical Systems*, 1st ed., F. Farokhi, Ed. Springer Singapore, 2020.

[9] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-aware location sharing with deep reinforcement learning," in *IEEE Workshop on Information Forensics and Security (WIFS)*, Delft, The Netherlands, Dec 2019.

[10] ——, "Privacy-aware time-series data sharing with deep reinforcement learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 389–401, 2021.

[11] ——, "Privacy-cost trade-off in a smart meter system with a renewable energy source and a rechargeable battery," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, UK, May 2019, pp. 2687–2691.

[12] B. Rassouli and D. Gündüz, "On perfect privacy," *IEEE Journal on Selected Areas in Information Theory*, pp. 1–1, 2021.

[13] Z. Li, T. J. Oechtering, and D. Gündüz, "Privacy against a hypothesis testing adversary," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1567–1581, June 2019.

[14] Y.-X. Wang, J. Lei, and S. E. Fienberg, "On-average kl-privacy and its equivalence to generalization for max-entropy mechanisms," *Int.l Conf. on Privacy in Statistical Databases*, 2016.

[15] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Active privacy-utility trade-off against a hypothesis testing adversary," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2021, pp. 2660–2664.

[16] B. Rassouli and D. Gündüz, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 594–603, 2020.

[17] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "A tunable measure for information leakage," in *2018 IEEE Int'l Symp. Inf. Theory (ISIT)*, June 2018, pp. 701–705.

[18] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *2016 Annual Conference on Information Science and Systems (CISS)*, 2016, pp. 234–239.

[19] S. A. Osia, B. Rassouli, H. Haddadi, H. R. Rabiee, and D. Gündüz, "Privacy against brute-force inference attacks," in *2019 IEEE Int'l Symp. Inf. Theory (ISIT)*, July 2019, pp. 637–641.

[20] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, "From the information bottleneck to the privacy funnel," in *2014 IEEE Information Theory Workshop (ITW 2014)*, 2014, pp. 501–505.

[21] A. Tripathy, Y. Wang, and P. Ishwar, "Privacy-preserving adversarial networks," in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2019, pp. 495–505.

[22] J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy-preserving multiobjective sanitization model in 6G IoT environments," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5340–5349, 2021.

[23] C.-W. Lin, T.-P. Hong, and H.-C. Hsu, "Reducing side effects of hiding sensitive itemsets in privacy preserving data mining," *TheScientificWorldJournal*, vol. 2014, p. 235837, 04 2014.

[24] C.-W. Lin, T.-Y. Wu, P. Fournier Viger, G. Lin, J. Zhan, and M. Vozňák, "Fast algorithms for hiding sensitive high-utility itemsets in privacy-preserving utility mining:," *Engineering Appl. of AI*, vol. 55, pp. 269–284, 10 2016.

[25] J. C.-W. Lin, P. Fournier-Viger, L. Wu, W. Gan, Y. Djenouri, and J. Zhang, "PPSF: An open-source privacy-preserving and security mining framework," in *2018 IEEE Int'l Conf. on Data Mining Workshops (ICDMW)*, 2018, pp. 1459–1463.

[26] J. M.-T. Wu, G. Srivastava, A. Jolfaei, M. Pirouz, and J. C.-W. Lin, "Security and privacy in shared hitlcps using a ga-based multiple-threshold sanitization model," *IEEE Tran. on Emerging Topics in Comput. Intel.*, vol. 6, no. 1, pp. 16–25, 2022.

[27] G. Smith, "On the foundations of quantitative information flow," in *Foundations of Software Science and Computational Structures*, L. de Alfaro, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 288–302.

[28] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1625–1657, 2020.

[29] G. Giaconi and D. Gündüz, "Smart meter privacy with renewable energy and a finite capacity battery," in *IEEE Int. Workshop on Sig. Proc. Advances in Wireless Communications (SPAWC)*, July 2016, pp. 1–5.

[30] W. Zhang, M. Li, R. Tandon, and H. Li, "Online location trace privacy: An information theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 235–250, Jan 2019.

[31] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 129–142, Jan 2018.

[32] J. Liao, L. Sankar, V. Y. F. Tan, and F. du Pin Calmon, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Trans. on Inform. Forensics and Security*, vol. 13, no. 4, pp. 1058–1071, 2018.

[33] M. Shoaib, H. Scholten, P. J. M. Havinga, and O. D. Incel, "A hierarchical lazy smoking detection algorithm using smartwatch sensors," in *IEEE Int'l Conf. on e-Health Networking, Applications and Services*, 2016, pp. 1–6.

[34] Z. Huang, L. Wang, G. Blaney, C. Slaughter, D. McKeon, Z. Zhou, R. J. K. Jacob, and M. C. Hughes, "The tufts fnirs mental workload dataset and benchmark for brain-computer interfaces that generalize," in *Proceedings of the Neural Information Processing Systems (NeurIPS) Track on Datasets and Benchmarks*, 2021.

[35] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, S. Halevi and T. Rabin, Eds. Springer Berlin Heidelberg, 2006.

[36] S. Yoo, M. Shin, and D. Lee, "An approach to reducing information loss and achieving diversity of sensitive attributes in k-anonymity methods," *Interact J Med Res*, vol. 1, no. 2, Nov 2012.

[37] N. Saleheen, S. Chakraborty, N. Ali, M. M. Rahman, S. M. Hossain, R. Bari, E. Buder, M. Srivastava, and S. Kumar, "msieve: Differential behavioral privacy in time series of mobile sensor data," *ACM Int'l Joint Conf. on Pervasive and Ubiquitous Comput.*, pp. 706–717, 2016.

[38] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: k-anonymity for location privacy," in *ACM Conference on Computer and Communications Security*, Sep. 2010.

[39] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *ACM Conf. on Computer and Commun. Security*, Oct. 2012, pp. 617–627.

[40] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *IEEE Symposium on Foundations of Computer Science*, Oct 2013, pp. 429–438.

[41] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 619–626, Mar. 2017.

[42] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 504–512.

[43] V. Bindschaedler and R. Shokri, "Synthesizing plausible privacy-preserving location traces," in *IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 546–563.

[44] M. Sun and W. P. Tay, "Inference and data privacy in IoT networks," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2017, pp. 1–5.

[45] M. A. Erdogdu and N. Fawaz, "Privacy-utility trade-off under continual observation," *IEEE Int'l Symp. Inf. Theory*, pp. 1801–1805, June 2015.

[46] S. Song and K. Chaudhuri, "Composition properties of inferential privacy for time-series data," in *Allerton Conference on Communication, Control, and Computing (Allerton)*, 2017, pp. 814–821.

[47] N. Tishby, F. Pereira, and W. Bialek, "The information bottleneck method," *Proceedings of the 37th Allerton Conference on Communication, Control and Computation*, vol. 49, 07 2001.

[48] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," *Proc. VLDB Endow.*, vol. 7, no. 12, p. 1155–1166, aug 2014. [Online]. Available: https://doi.org/10.14778/2732977.2732989

[49] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, "Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy," *IEEE Tran. on Depend. and Secure Comput.*, vol. 15, no. 4, pp. 591–606, 2018.

[50] X. Ren, L. Shi, W. Yu, S. Yang, C. Zhao, and Z. Xu, "Ldp-ids: Local differential privacy for infinite data streams," ser. SIGMOD '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 1064–1077. [Online]. Available: https://doi.org/10.1145/3514221.3526190

[51] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy," in *IEEE Symposium on Security and Privacy*, May 2011, pp. 247–262.

[52] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, "Quantifying differential privacy in continuous data release under temporal correlations," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 7, p. 1281—1295, July 2019.

[53] D. J. Mir, "Information-theoretic foundations of differential privacy," in *International Symposium on Foundations and Practice of Security*. Springer, 2012, pp. 374–381.

[54] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *2011 IEEE 24th Computer Security Foundations Symposium*, 2011, pp. 191–204.

[55] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy: on the trade-off between utility and information leakage," in *Int'l Work. on Formal Aspects in Sec. and Trust*. Springer, 2011, pp. 39–54.

[56] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3679–3695, May 2018.

[57] P. Venkitasubramaniam, "Privacy in stochastic control: a Markov decision process perspective," in *2013 51st Annual Allerton Conf. Commun., Control, and Comput. (Allerton)*, Oct 2013, pp. 381–388.

[58] D. P. Bertsekas and S. E. Shreve, *Stochastic Optimal Control: The Discrete-Time Case*. Belmont, CA: Athena Scientific, 2007.

[59] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, 1st ed. USA: John Wiley & Sons, Inc., 1994.

[60] C. H. Papadimitriou and J. N. Tsitsiklis, "The complexity of markov decision processes," *Mathematics of Operations Research*, vol. 12, no. 3, pp. 441–450, 1987.

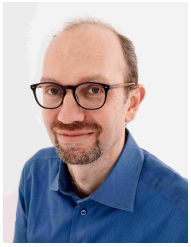
[61] N. Saldi, T. Linder, and S. Yüksel, *Approximations for Partially Observed Markov Decision Processes*. Cham: Springer Int'l Publishing, 2018, pp. 99–123.

[62] D. Barber and F. Agakov, "The im algorithm: a variational approach to information maximization," in *NIPS 2003*, 2003.

[63] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed. The MIT Press, 2018.

[64] I. Grondman, L. Busoniu, G. A. D. Lopes, and R. Babuska, "A survey of actor-critic reinforcement learning: Standard and natural policy gradients," *IEEE Trans. Syst., Man, Cybern., Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1291–1307, Nov 2012.

Ecenaz Erdemir (Member, IEEE) is an Applied Scientist at Amazon Web Services (AWS) AI, New York, NY, U.S.A. She received her B.S. and M.S. degrees in Electrical and Electronics Engineering from Middle East Technical University (METU), Ankara, Turkey, in 2014 and 2017, respectively. She received her Ph.D. degree in the Electrical and Electronic Engineering Department at Imperial College London, London, U.K., in 2022. Her current research interests are information security, cybersecurity, data privacy, machine learning, information theory and decision theory.



Pier Luigi Dragotti (Fellow, IEEE) received the Laurea degree (summa cum laude) in electronic engineering from the University of Naples Federico II, Naples, Italy, in 1997, and the M.S. degree in communications systems and the Ph.D. degree from the Swiss Federal Institute of Technology of Lausanne (EPFL), Switzerland, in 1998 and in April 2002, respectively. He has held several visiting positions, in particular, he was a Visiting Student at Stanford University, Stanford, CA, USA, in 1996; a Summer Researcher at Bell Labs, Lucent Technologies, Murray Hill, NJ, USA, in 2000; a Visiting Scientist with the Massachusetts Institute of Technology (MIT) in 2011; and a Visiting Scholar at Trinity College, Cambridge, UK, in 2020. Before joining Imperial College London (ICL) in November 2002, he was a Senior Researcher at EPFL working on distributed signal processing for the Swiss National Competence Center in Research on Mobile Information and Communication Systems. He is currently Professor of Signal Processing with the Electrical and Electronic Engineering Department, ICL. His research interests include sampling theory and its applications, computational imaging, and sparsity-driven signal processing. Dr. Dragotti was an Elected Member of the IEEE Image, Video and Multidimensional Signal Processing Technical Committee as well as an Elected Member of the IEEE Signal Processing Theory and Methods Technical Committee and the IEEE Computational Imaging Technical Committee. In 2011, he was awarded the Prestigious ERC Starting Investigator Award. He was also IEEE SPS Distinguished Lecturer (2021-2022), the Editor-in-Chief of the IEEE TRANSACTIONS ON SIGNAL PROCESSING (2018–2020), the Technical Co-Chair of the European Signal Processing Conference in 2012, and an Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING from 2006 to 2009.

Deniz Gündüz (Fellow, IEEE) received the B.S. degree in electrical and electronics engineering from METU, Turkey in 2002, and the M.S. and Ph.D. degrees in electrical engineering from NYU Tandon School of Engineering (formerly Polytechnic University) in 2004 and 2007, respectively. Currently, he is a Professor of Information Processing in the Electrical and Electronic Engineering Department at Imperial College London, UK, where he also serves as the deputy head of the Intelligent Systems and Networks Group. He has held visiting/part-time positions at the University of Modena and Reggio Emilia, University of Padova, Princeton University, Stanford University and CTTC. His research interests lie in the areas of communications and information theory, machine learning, and privacy. Dr. Gündüz is a Fellow of the IEEE, and a Distinguished Lecturer for the IEEE Information Theory Society (2020-22). He serves in editorial roles for the IEEE Transactions on Information Theory, IEEE Transactions on Communications, IEEE Journal on Selected Areas in Communications (JSAC), and the IEEE Transactions on Wireless Communications. He is the recipient of the IEEE Communications Society - Communication Theory Technical Committee (CTTC) Early Achievement Award in 2017, Starting (2016) and Consolidator (2022) Grants of the European Research Council (ERC), and several best paper awards.