Privacy preservation using game theory in e-health application

Arbia Riahi Sfar, Enrico Natalizio, Sahbi Mazlout, Yacine Challal, Zied Chtourou

Privacy preservation using game theory in e-health application

1st Arbia RIAHI SFAR
TICAD Lab.
Military Academy of Tunisia
Nabeul, Tunisia
ORCID: 0000-0002-5739-1343

2nd Enrico NATALIZIO
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
ORCID: 0000-0001-8553-5722

3rd Sahbi MAZLOUT
TICAD Lab.
Military Academy of Tunisia
Nabeul, Tunisia
email address or ORCID

4th Yacine CHALLAL
dept. name of organization (of Aff.)
name of organization (of Aff.)
Alger, Algeria
ORCID: 0000-0002-9237-6210

5th Zied CHTOUROU
TICAD Lab.
Military Academy of Tunisia
Nabeul, Tunisia
ORCID: 0000-0001-7154-6906

***Abstract*—In the domain of the new e-health applications, the ubiquitous nature of intelligent devices raises legitimate questions about the privacy of persons, and how to cope with the heterogeneity of user and application requirements in terms of security services. This requires the development of adaptive, context-aware and user-centric security solutions. Recent e-health applications (M2M/IoT/Web) permit remote monitoring of patient health, medical treatments, fitness information and parameters, alarm triggering, etc. Since the monitored device is tightly related to a human being, new changes arise regarding communications facilities constraints, private data protection, trust relationships, etc. In this work, we propose a Markovian game between data holder and data requester, in a weight loss program, to protect data privacy. We aim to reach a compromise between privacy concessions made by data holder and incentive motivation proposed by data requester. Finally, we show numerical results of executed experiments to evaluate the proposed model.**

***Index Terms*—Privacy, Internet of things, e-health, game theory, Markovian process.**

I. Introduction

E-health improves both personal and public health, and assists individuals in self-monitoring, disease management and access to health records. An e-health system involves different participants such as patients, research professionals, clinicians, governments, etc. In the new healthcare applications, novel technologies may play a key role. Examples may include medical mobile applications, wearable intelligent objects capturing patient's health data (blood pressure, temperature, weight...), tabs kept by hospitals to log location of personnel, etc. [1]. The usage of new means such as M2M (Machine-to-Machine), IoT (Internet of Things) and Web means enhances e-health applications by integrating new technologies in data sensing, data analysis and area networking. This leads to efficiency gains in health service methods, individual's control, care quality, etc. [2]. The use of electronic devices, connected to a private or public cloud, for data capture and/or supervision goals may generate new challenges [3]. Interactions between humans and devices may increase power consumption and require battery changes and patient's mobility must be considered with regard to device location. And, data exchange over a public network may create privacy dilemma.

In ETSI uses cases presented in [4], the main objectives of new e-health applications include remote monitoring of patient health and fitness information, triggering alarms when critical conditions are detected, controlling medical treatments or parameters, and so on. The analysis identifies actors and their roles for each use case and debates connectivity, interoperability, security and standardization issues. Authors specifically described the instance of personal fitness and health improvement. Examples of applications in this case may concern record health and fitness indicators during exercise sessions (heart and breathing rates, energy consumption, fat burning rate), monitoring the frequency and time of workouts, controlling the exercises intensity, running distances, etc. New challenges about using and securing mobile devices within IoT operations take place and many concerns can arise due to the storage and exchange of sensitive information through connected devices [5]. The expected increase of the number of connected devices will raise new security issues regarding the generated information, the number of input/outputs of a single system, and the numerous interactions between devices and/or humans. Also, data transmitted through wireless networks can be easily accessed by attackers, and even be destroyed, intercepted or altered. Unfortunately, classical and common solutions such as encryption methods are not suitable to solve the security concerns discussed

previously due to the limited capabilities of connected devices [**?**]. many intelligent objects have insufficient onboard memory and processing capacity to handle standard protocols. They may suffer from power limitation to execute all the algorithmic computations needed for data encryption/decryption. With the integration of new technologies, security and privacy concerns involve a strong interaction of objects and humans. In e-health scenarios, the connected devices became able to act on human's behalf, and can make their decision autonomously. Node's behavior may be cooperative, selfish, malicious, curious, etc., which generates many security challenges during the decision making process [6]. This led many researchers to use game theory to formulate actor's interactions in e-health security scenarios where they may be modeled as attackers/defenders. This is explained by the large number of mathematical tools available for multi-user strategic decision making. They are used to develop formal decision making, algorithms and attacker behavior prediction [7].

Our contribution is threefold. First, we identify privacy concerns in an IoT based e-health system. Second, we propose a game model for privacy protection based on Markovian process. Third, we validate our theoretical findings with numerical results. We propose an e-health privacy model based on three main elements: ETSI uses cases (e-health applications for M2M communications); smart health platform architecture of Continua Health Alliance (industry consortium promoting e-health and guaranteeing end-to-end interoperability); and a common e-health scenario involving four actors: participants, coaches, clinicians and commercials.

The remaining of this paper is organized as follows. Section II highlights the use of game theory to solve privacy questions and depicts the most important related works. Section III describes the overall architecture of the proposed solution. Section IV presents the game model mathematical formulation and numerical results.

II. Related work

In the last few years, numerous research efforts focus on security and privacy using game theory, but limited efforts deal with e-health applications. This section overviews some of the noteworthy works realized by various researchers. In [8], authors proposed a game theoretical approach with a two-stage channel allocation scheme: BBN-stage for inter-WBANs, and WBAN-stage for intra-WBAN communications to solve distributed interference mitigation problem in Body-to-Body Networks. Their work is based on the best-response approach to compute the Nash Equilibria in a distributed fashion. The objective of this work is limited to interference mitigation problem and does not consider privacy and trust aspects. In [9], authors proposed a radio resource allocation scheme for wireless body area networks (WBANs). They focused on the communications in beyond-WBANs, and debated the transmission scheme in case of a large number of gateways associating with one base station of medical centers. They provide a priority-aware pricing-based capacity sharing design by considering the quality of service (QoS) constraints for different gateways. This work focuses on QoS concerns only and is not interested in security questions related to private data protection and human/object trust management. In [10], authors proposed a new e-health model combined with cloud computing platform to offer health related services in IoV (Internet of Vehicles) environment on-the-fly. They used a game theory model where vehicles act as players and tend to form and split coalitions to access e-health services. Vehicles are represented as stochastic reward nets (SRNs), and a new payoff function is designed for them taking into consideration coalition among the players in the game. Although its originality, this work did not discuss security questions in e-health domain. In [11], authors designed a framework for an IoT-based smart health system based on existing technology standards and communication protocols. Although their interest to solving interoperability problems, they did not discussed privacy issues in sensitive e-health scenarios. In[12], authors proposed a power control algorithm under a non-cooperative game theoretic framework to schedule data transmission in mobile hospital environments. They solved the problem of network-level optimal capacity using a game strategy based on the best-response-dynamics algorithm.

In [13], authors proposed a Markovian game-theoretic model for adaptive security in IoT-based e-health applications. They introduced four strategies to conceive their game model related to the smart object energy, the channel state, the memory space and the intruder. They focused on the compromise between BAN capabilities and smart objects lifetime; and used an adaptive security policy based on authentication to evaluate their model. From a security point of view, authors analysis is limited to intrusion concerns using witness based detection methods. We consider this work very inspiring in the development of our model but we state that data sensitivity, privacy and trust concerns, frequently present in IoT-based e-health context, were not sufficiently debated. Moreover, actions and transitions of each player were not explicitly defined in their game model. In a previous work [6], we proposed a privacy preserving solution in ITS (Intelligent Transportation Systems) context relying on a game theory model between two actors to protect private data using an incentive motivation against a privacy concession, or leading an active attack.

III. E-health solution architecture and privacy preservation

In an e-health scenario, it is meaningful to make the following medical pre-assumptions. Clinical operations must include initial medical assessment, regular monitoring, measurement, and counseling by healthcare professionals Also, we suppose that scenario may include

the following parameters: medical report, behavior modification, diet and nutrition, physical activity, time, etc. Participants create their own electronic health record through health measures including program information, preferences, visit planning, tracking data, social engagement and progress. Unquestionably, this type of healthcare services generates an increasing amount of data and evidence since electronic health records are used to trace people's health information.

This motivates the emergence and the progress of health data management research and practice [7], and the use of an approved architecture for big data. The smart health platform architecture of Continua Health Alliance has followed H.810 design guidelines and was approved by ITU [14]. It allows a wide range of personal/clinical health devices to be used or interchanged in any setting. Furthermore, due to the performance of communication means, novel technologies can assure automatic and precise data capture, and real-time updates of health record. Accordingly, the overall architecture of the proposed e-health solution is shown in figure 1 and includes three main parts: personal health device (actuators, sensors, etc.), application hosting device (PC, personal health system, smartphone, aggregator, etc.) and healthcare service provider (clinicians, commercials, etc.), interacting as illustrated in table I.

In the big data era, the key to developing a successful e-health application is to handle efficiently a sizable amount of data, that may contain sensitive information about individuals. An increasing concern about privacy threats posed by data affluence and device ubiquity takes place. Individuals have to be sure that their data, collected for a specific purpose, are not reused for another purpose without their permission. Also, they have to avoid data inference and re-identification risks by choosing trusted service provider. Privacy is then imperative to protect sensitive information used during data handling, and finding a compromise between novelty and data protection without risking over-reaction.

To handle privacy issues, all phases of the big data value chain must be considered including acquisition/collection, analysis, storage, and use. In practice, two solutions are possible: privacy by design, and privacy enhancing technologies [15]. The concept of privacy by design takes place at the beginning of the development of a product or service, and denotes the integration of privacy protection into both technology (computer chips, networking platforms, etc.) and organizational policies (privacy impact assessments). Embedding privacy enhancing technologies permits to avoid personal data compromise, rebuild trust between users and service providers, and consider the dimension and emerging big data environment. Available techniques to ensure privacy are summarized in [15] and include anonymization, encryption, security and accountability controls (granular access control, policy enforcement, accountability and audit, data provenance), transparency, consent, ownership, and control (consent, privacy preferences, sticky policies, personal data stores). Authors conclude that the road to ensure big data privacy is still long and hard, as data amount is growing every day and privacy preserving mechanisms are not following accordingly.

Online privacy problem is a defying combination of information imbalance, external forces (political, social...), structural invisibility, technological components, complex privacy preferences, and unreliable modes of communication [16]. Therefore, game theory has lately emerged as a mean for modeling interactions of multiple rational selfish entities with conflicting interests, and for calculating stable system points (equilibrium) from which no entity can obtain additional benefit [17]. Depending on information's nature, game players types, actions and final goals, many categories of security games may be distinguished (deterministic, zero-sum, Stackelberg, repeated, stochastic, incomplete information, etc.) to solve security problems as privacy protection and trust management in IoT-based networks [7].

Figure 1 illustrates the proposed solutions, where the personal e-health device plays the role of data provider, the hosting device of the application plays the role of data collector. Healthcare service provider plays the role of data user with two sub-roles (data miner and decision maker). The game model is developed between data collector and data provider (likewise for data user and data collector) when attempting to access private data. This architecture permits the game model implementation including its actors, actions, payoffs, utility functions and Nash equilibrium, as described in the following sections.

To solve privacy problems in data sharing (PPDM/PPDP), we need to consider the following aspects. First, in the data publishing/sharing model, questions concern (1) publishing data table or statistical values; and (2) results of data analysis (classifiers, regression models...). Usable techniques include anonymization (k-anonymity (PPDP)) and randomized approach (Differential privacy (PPDM)). Second, in the database-querying model (searches, recommendation, diagnosis, etc.), the query contains user's private information that need to be protected. Usable techniques include Multiparty Computation (MPC) techniques (high computational cost), and query auditing techniques to check database-privacy preservation by examining past data publishing (high computational cost). Third, the data integration model is used to enhance the knowledge quality they can obtain from their data. Solutions include MPC (to obtain statistical data) and Ensemble / data aggregation (used if the data-mining for integrated data is desired and statistical data are available).

Table I
E-HEALTH SYSTEM INTERACTIONS IN WEIGHT LOSS PROGRAM SCENARIO [2].

System elements		Interactions
Personal Health Device	Application Hosting Device	Ensuring that data user knows exact measurements values, time and place; and that this critical data are not lost during transportation and handling.
Application Hosting Device	Device connectivity	Device observations (one-way): transmission of measurement(s) between personal health gateway and health/fitness service.
		Questionnaires: patient reported outcome measures, or questionnaires, used in clinical setting to collect information directly from the patient.
		Consent management: enabling patients to authorize healthcare providers to access and share sensitive information.
		Capability exchange: reducing the amount of information that must be pre-configured on e-health device to obtain interoperability.
		Authenticated Persistent Session: enabling a persistent secure channel in the cellular environment where bandwidth, power, and IP resources may be limited and/or intermittent.
Application Hosting Device	E-health records	Carrying personal healthcare monitoring information to electronic medical record systems (measurements captured by devices).
Application Hosting Device	Medical systems/providers	Enabling healthcare documents to be shared over a wide area network between hospitals and care providers.

IV. PROPOSED MODEL

A. Game assumptions

In the following, we make the following assumptions:

- The game involves two types of players: *Data Holder* (DH) and *Data Requester* (DR).
- Players are rational and DHs grant high interest to privacy preservation of their data utility.
- The game evolution depends on the negotiation or the attack steps/parameters between DR and DH.
- Actions are sequential, and the game is such that only one player moves at any point of time.
- Previous action results are included in system state.
- DH ignore DR's strategy, and can only predict it from previous action results, which are assumed to be observable by him/her.
- DR can DH and DR have dependent interests and aim to maximize their benefits.
- DH has the convenient decision making mechanism to assure a minimal privacy damage.

B. Model description

1) Actors and roles: In the proposed solution, two scenarios can be distinguished. In the first scenario, data provider is the personal health device which owns sensitive data (weight scale, glucose readings, blood pressure, pulse oximetry, etc.) and, therefore plays the role of DH. The application hosting device is the data collector and plays the role of DR. In the second scenario, the application hosting device owns private data (DH), and the data user is represented by e-health service provider, commercial or decision maker who attempts to access private data (DR). We notice that in both scenarios, except different payoffs, players behave similarly when they play the same role (DH or DR). That means, data provider (personal health device) behaves in the same manner in the first scenario as data collector (application hosting device) behaves in the second scenario since both of them play the role of DH. In practice, we assume that the personal e-health device is the DH, the hosting device of the application is the data collector (DR) or the DH, the healthcare service provider is the data user (DR) with two sub-roles (data miner and decision maker). Then, it becomes possible to develop a game model where the data collector attempts to access private data hold by the data provider, and the data user aims to access private data owned by the data collector.

2) Data flow and sequence diagrams: The game proceeding is illustrated in figure 4 where we distinguish two different situations : *negotiation* and *attack*. In the first case, DR may iterate the negotiation state until reaching a satisfying agreement or abandon the game. In the second case, the DR carries an attack to compromise DH and gain access to private data, or abandon the game for communication features or demotivation reasons. Sequence diagrams in figure 2 depict behavioral aspects of a system and present the control flow among actors. In the the first situation, we highlight the different steps of the privacy game evolution in function of privacy concession and incentive motivation. In the second situation, we consider the attack case where the DR is malicious.

3) Strategies parameters: DH may provide or not private data of multiple sensors to DR in function of game evolution. Player's strategies are described in a Markovian process by transitions between states depending on five parameters: (1) energy and communication facilities, (2) DR type, (3) data privacy concession, (4) incentive motivation, and (5) attack/intrusion presence. The first parameter is related to energy and communication facilities (battery level, channel state, memory state, etc.). To simplify ideas, the node ensures that communication facilities are "$favorable$" when all of the facilities are verified.

The second parameter refers to attack capability detection. We assume that external attackers are strong

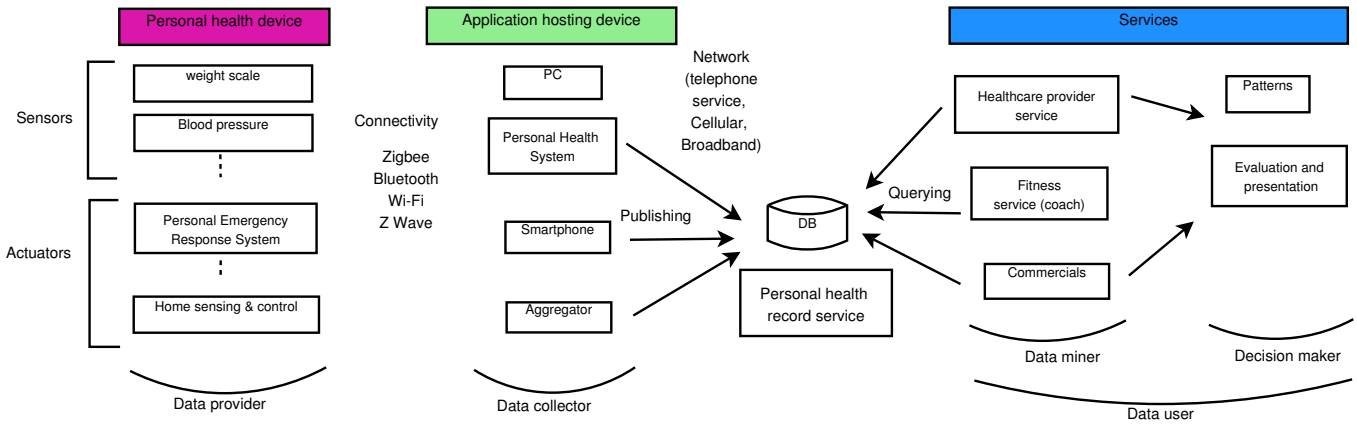


Figure 1. E-health solution components [18].

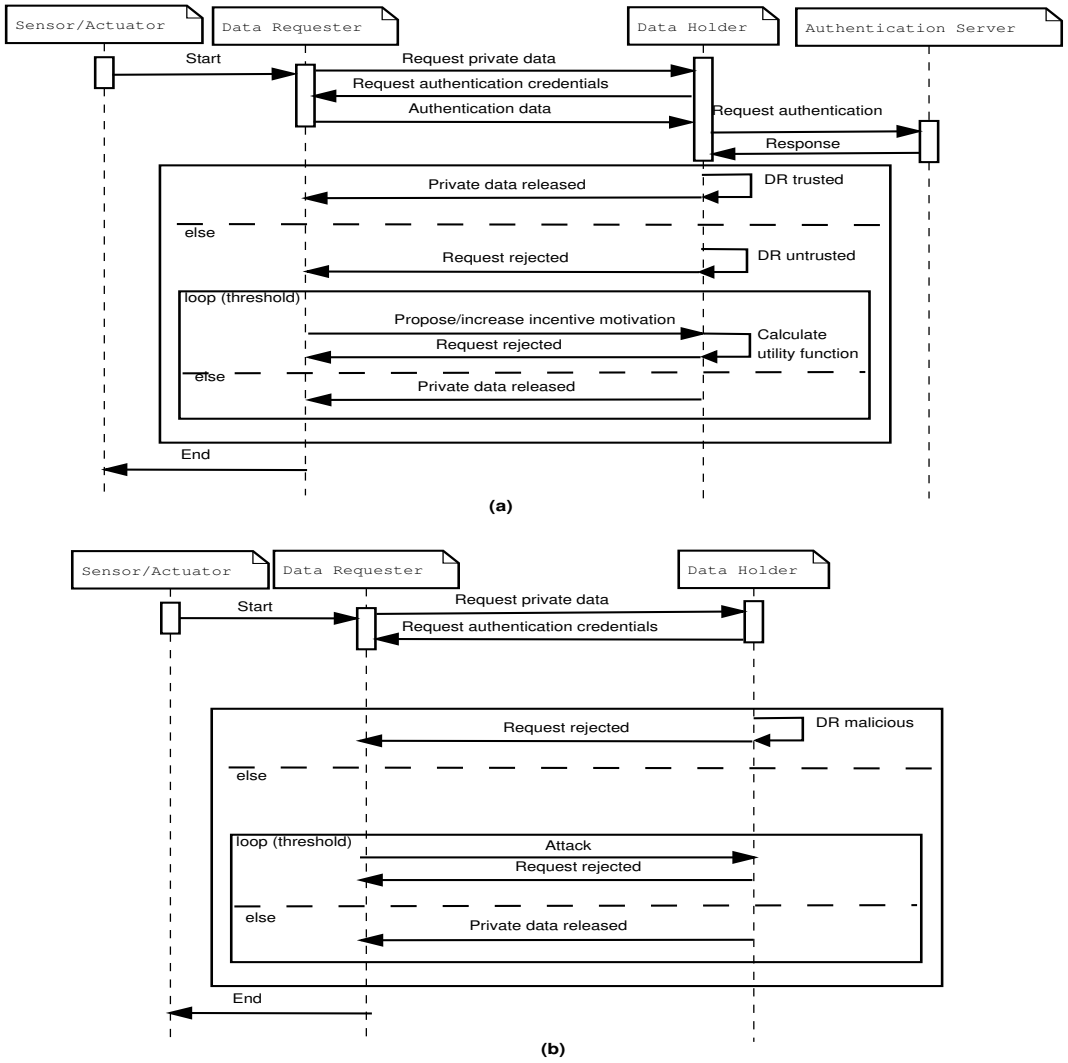


Figure 2. Sequence diagrams of the privacy game ((a): DR trusted/curious, (b): DR malicious).

Table II
GAME STRATEGIES

Transition	Transition probability	Condition	Condition Probability
Strategy 1 (adapting to the communication facilities) : DH switches to the *passive* mode if one of the parameters of *communication facilities* is not acceptable and to *active* mode if all the parameters are acceptable.			
Passive →Active	$P_{P\Longrightarrow A}=\begin{cases} p_c \\ 1-p_c \end{cases}$	$favorable$ $unfavorable$	p_c^h $1-p_c^h$
Active → Passive	$P_{A\Longrightarrow P}=\begin{cases} {p'}_c \\ 1-{p'}_c \end{cases}$	$favorable$ $unfavorable$	p_c^h $1-p_c^h$
Strategy 2 (adapting to the attack): DH switches to active/passive mode depending on intrusion detection result.			
Passive →Active	$P_{P\Longrightarrow A}=\begin{cases} p_a \\ 1-p_a \end{cases}$	$no\ attack$ $attack$	p_a^h $1-p_a^h$
Active → Passive	$P_{A\Longrightarrow P}=\begin{cases} p'_a \\ 1-p'_a \end{cases}$	$no\ attack$ $attack$	p_a^h $1-p_a^h$
Strategy 3 (adapting to the adversary) : DH may switch to the *passive/active* mode if DR is untrusted (*reject*). He/she switches to the *active* mode (*disclose*, or *negotiate*) if DR is trusted.			
Passive →Active	$P_{P\Longrightarrow A}=\begin{cases} p_r \\ 1-p_r \end{cases}$	$adversary\ trusted$ $adversary\ untrusted$	p_r^h $1-p_r^h$
Active → Passive	$P_{A\Longrightarrow P}=\begin{cases} p'_r \\ 1-p'_r \end{cases}$	$adversary\ trusted$ $adversary\ untrusted$	p_r^h $1-p_r^h$
Strategy 4 (adapting to the incentives) : DH may switch when the proposed incentives are not interesting.			
Passive →Active	$P_{P\Longrightarrow A}=\begin{cases} p_i \\ 1-p_i \end{cases}$	$Incentive\ value\ favorable$ $Incentive\ value\ unfavorable$	p_i^h $1-p_i^h$
Active → Passive	$P_{A\Longrightarrow P}=\begin{cases} p'_i \\ 1-p'_i \end{cases}$	$Incentive\ value\ favorable$ $Incentive\ value\ unfavorable$	p_i^h $1-p_i^h$
Strategy 5 (adapting to the privacy) : DH switches to the *passive* mode if the data loss is higher than a fixed threshold and to the *active* mode otherwise.			
Passive →Active	$P_{P\Longrightarrow A}=\begin{cases} p_p \\ 1-p_p \end{cases}$	$concession$ $no\ concession$	p_p^h $1-p_p^h$
Active → Passive	$P_{A\Longrightarrow P}=\begin{cases} p'_p \\ 1-p'_p \end{cases}$	$concession$ $no\ concession$	p_p^h $1-p_p^h$

and can overhear, intercept and generate any message but do not know the defense strategy of DH. As many intrusion detection systems exist and are able to detect attacks and makes DH aware of them, we consider only the possibility of disclosing data by DH in intrusion situations. Intrusion detection is out of the scope of our work, then we suppose the existence of a suitable system, able to detect attacks and makes DH aware of them.

The third parameter is associated with the adversary type. According to the players behavior, we distinguish three types of adversaries : (1) $Regular-Trusted$ (RT), registered in e-health system and authorized to access private data (coach, clinicians, etc); (2) $Curious-Trusted$ (CT), registered but attempts to access private data by proposing incentive compensation, (3) $Curious-Untrusted$ (CU), unregistered and attempts to access private data by proposing incentive compensation, or (4) $Malicious-Untrusted$ (MU), unregistered and leads an attack to access private data. From DR perspective, adversary belongs imperatively to the first category (RT).

The fourth parameter describes the incentive motivation offered by DR to DH . It depends on external market conditions which indicate how valuable the data is to the holder and the incentives value proposed by DR in the negotiation phase. This motivation may influence DH to change his/her initial intention by making privacy concession.

The fifth parameter presents privacy preferences and data sensitivity loss of DH. Privacy preferences may be used when a patient authorizes only specific doctors to view or modify his/her health records. The privacy loss of disclosed data can be perceived when data provider makes privacy concession by decreasing privacy preferences and disclose private data. Each player has his/her own strategy to switch between states through available actions. For each strategy, we define the transition probabilities between states according to game parameters.

V. GAME FORMULATION

A. Markovian process

1) System components and states: The objective is to find the optimal defense strategy for DH to preserve data privacy over a serial of related situations. Through a set of strategic operations, DH can adaptively maximize

State	Description
OoP (Out of Process)	The player is waiting for communication facilities improvement (battery charging, channel availability, etc.).
Idl (Idle)	Communications facilities are favorable and the player is ready for playing.
Aut (Authenticate)	Authentication phase used to fix privacy settings of DH.
Neg (Negotiate)	Both players participate in a negotiation for buying /selling private data.
Att (Attack / defend)	Both players participate in an attack / defense process to access / protect private data.
Rel (Release)	End of the game by releasing private data.
Rej (Reject)	End of the game by rejecting access to private data.
Com (Compromise)	DH is compromised by DR and private data are released.

Table III
MARKOVIAN PROCESS STATES.

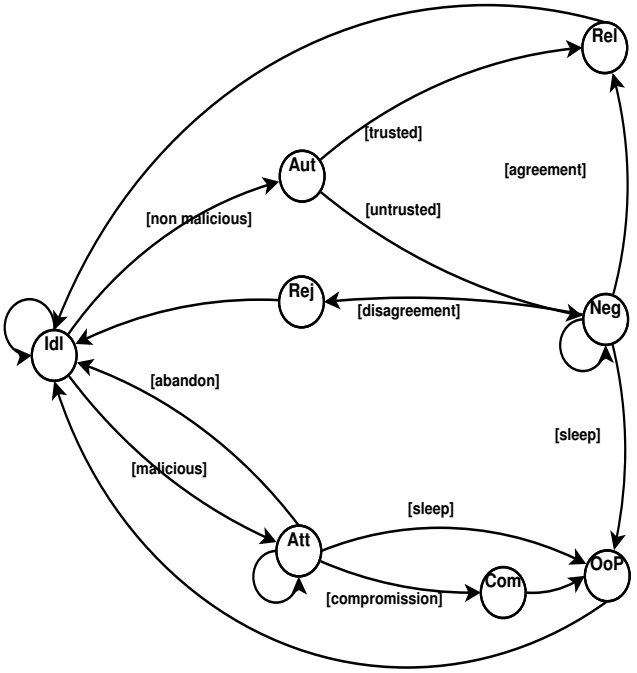


Figure 3. State diagram representations of the game from the DH perspective

his/her utility to protect private data, and DR (curious or malicious) aims at minimizing DH's utility. We define eight states for each player (table III) grouped into two macro-states: *active* and *passive*. Each player makes one action to reach one state.

In the *active* mode, DH participates to the game and may *authenticate* DR, *negotiate* incentive motivations and privacy parameters, *release* his/her private data, defend him/her privacy against DR *attack*, or be *compromised*.

In the *passive* mode, the node does not participate to the game when it is in the *idle* state, or due to communication features limitations (*out of process*), or by rejecting (*reject*) the offer proposed by DR.

2) Game strategies: For simplicity, we assume that DR have the same probability to belong to any of the four player categories, which means that any node has the probability of $\frac{1}{4}$ to be $Regular-Trusted$, $Curious-Trusted$, $Curious-Untrusted$ or $Malicious-Untrusted$. DH type is always a $Regular-Trusted$ node. DH's behavior is more challenging than DR since he/she has to find an equilibrium between privacy preferences and financial motivations.

In figure 3, when DR is a trusted player, negotiation and incentive motivation are not needed and transitions to the *Rel* state takes place. When DR is curious (trusted or untrusted) and attempts at accessing private data, he/she proposes an incentive motivation with respect of DH privacy preferences. When DR is malicious, he/she leads an attack against DH to access private data.

Table II details DH's game strategies variation among passive and active states, based on five parameters (subsection IV-B3), namely: c (energy and communication facilities), q (adversary type), p (data privacy), i (incentive motivation) and a (attack / intrusion).

Markovian process describes the system which states change over time, commonly called discrete time stochastic process. As changes are governed by a probability distribution, the next state depends only on the current system state. Every finite state in the Markovian process has at least one stationary distribution (also called steady state) which satisfies:

$$\pi = \pi P,\ with\ \sum_i \pi(i) = 1$$

Where $\pi(i)$ expresses the probability that Markovian process in state i, and $P = (P_{ij})$ is a $N \times N$ stochastic matrix specifying the transition rules. The power of the transition matrix gives interesting information about the evolution of the process.

We think that DH's behavior is more challenging than DR's since he/she has to find an equilibrium between privacy preferences and financial motivations. DR aims only at accessing private data and is not called to make privacy concessions. The Markov representation has the following state-space:

$$S = \{Idl, Aut, Rel, Rej, Com, OoP\} \cup \{(Neg, i) : i = 0, 1, ...\} \cup \{(Att, j) : j = 0, 1, ...\},$$

Any state of the form (Neg, i) ((Att, j) resp.) means that DH/DR has been negotiating (Attacking/Defending resp.) for i (j resp.) times.

3) Transition matrix: Figure 3 depicts the state diagram from DH perspective. For calculation needs, we consider the following probability values (a, b, c, d, e, f, g, h, and $k \in [0, 1]$) and transition matrix is :

$$P = \begin{array}{c} \\ Idl \\ Aut \\ Rel \\ Rej \\ Com \\ OoP \\ Neg \\ Att \end{array} \begin{array}{c} \begin{array}{cccccccc} Idl & Aut & Rel & Rej & Com & OoP & Neg & Att \end{array} \\ \begin{pmatrix} a & b & 0 & 0 & 0 & 0 & 0 & 1-(a+b) \\ 0 & 0 & c & 0 & 0 & 0 & 1-c & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & d & e & 0 & f & 1-(d+e+f) & 0 \\ g & 0 & 0 & 0 & h & k & 0 & 1-(g+h+k) \end{pmatrix} \end{array}$$

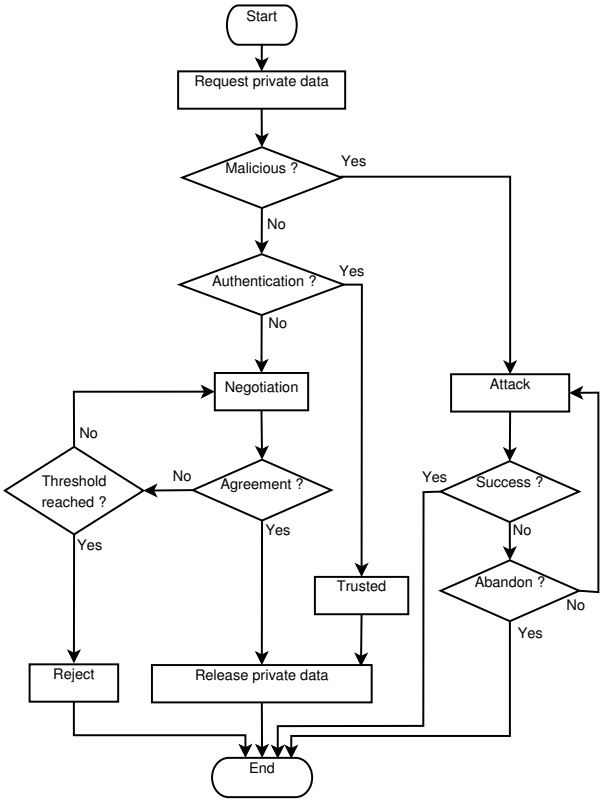


Figure 4. Flow Diagram of the privacy game.

Steady state probabilities are represented in figure 5 where we notice that for a low value of a ($a = 0.1$), probabilities of active states are high (favorable communication features). For high values of b (authentication), attack and compromising possibilities are limited. For high values of c (authentication), releasing probability is high, reject and negotiation probabilities ares low. In addition, DH decision depends on parameters d (intention of disclosure), e (intention of reject), f (intention of abandon), and $1-(d+e+f)$ (indecision). When d heighten, release probability increases and negotiation intention decreases. The system behaves inversely for parameter e. In attack scenario, DH decision depends on parameters g (attack intention), h (attack success), f (abandon intention), and $1-(g+h+k)$ (DR persistence). For high values of g, communications features are limited and the systems lasts log time in $Idle$ state. For high values of h, probability of DH compromising is high. Similarly, for high values of k, DH compromising and data release probabilities increase.

B. Utility functions

After observing the state at each stage, both players decide their actions for the current stage. DH controls the granularity of the released data to protect his/her context privacy. To reach final states, DH calculates utility function value to decide whether accept or reject current DR proposed offer. It reflects his/her ability to release private data against an incentive motivation. We construct U, the utility function of DH, composed of two sub-functions: a loss function, which returns the privacy concession; and a gain function, which represents the impact of the incentive motivation. We consider DH is interested in both privacy and incentive and we model the game utility function as defined in [19]:

$$U(p_{inc}, p_{priv}) = A[C + C_{inc} * h_{inc}(p_{inc}) + C_{priv} * h_{priv}(p_{priv})] + B;$$

where p_{inc} and p_{priv} are the probability of making privacy concession and the probability of accepting incentive motivation proposed by DR, h_{inc} and h_{priv} are functions of p_{inc} and p_{priv}. C_0, C_{inc} and C_{priv} are the intercept and marginal effects of $h_{inc}(p_{inc})$ and $h_{priv}(p_{priv})$ on DH's decision to disclose private data or reject. h_{inc} and h_{priv} can be any non-decreasing functions. A and B are external fixed costs. p_{inc} and p_{priv} are defined independently, but express the same event of disclosing private date when accepting incentive motivation [6]. Then, their values coincide:

$$p_f := p_{priv} = p_{inc};$$

For incentive model, we refer to [20]:

$$h_{inc}(p) = \lambda * \sqrt{p};$$

where λ is the data value to the DR.
For privacy model, we consider the proposal of [21]:

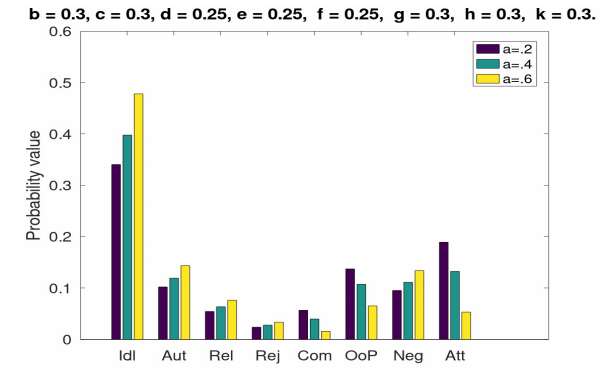
$$h_{priv}(p) = \alpha * ln(p + \beta) + \gamma;$$

where $\{\alpha, \beta, \gamma\} \in [0, 1]$ are privacy parameters.
Then utility function is given as follows:

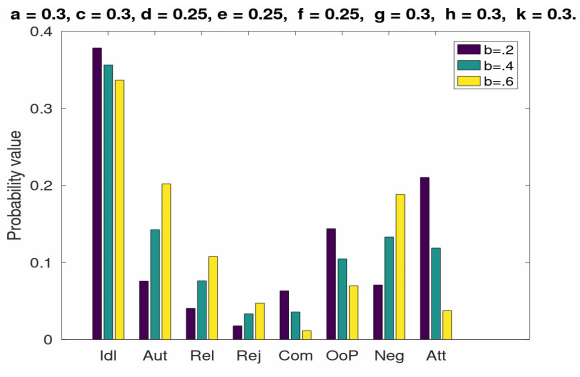
$$U(p) = C_0 + C_1 * h_{inc}(p_{inc}) - C_2 * h_{priv}(p)];$$

where $\{C_0, C_1, C_2\}$ are positive constants.

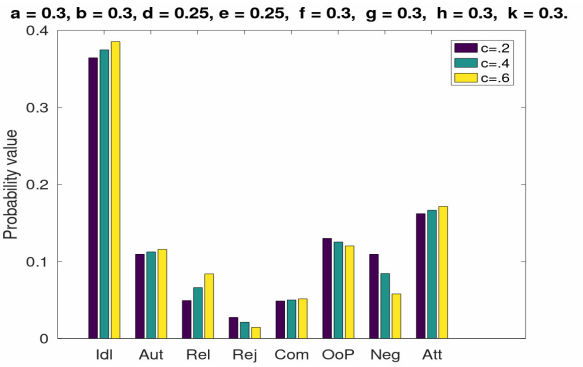
Figure 5. Steady states for variable game parameters



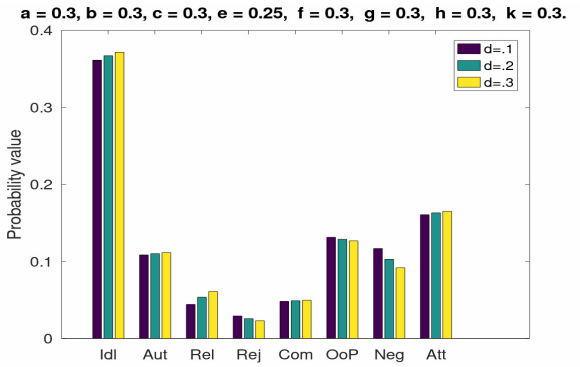
(a)



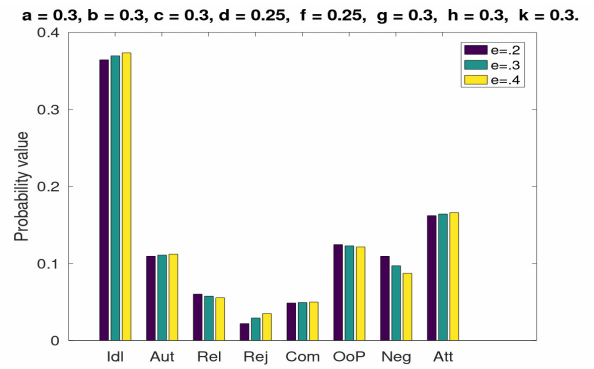
(b)



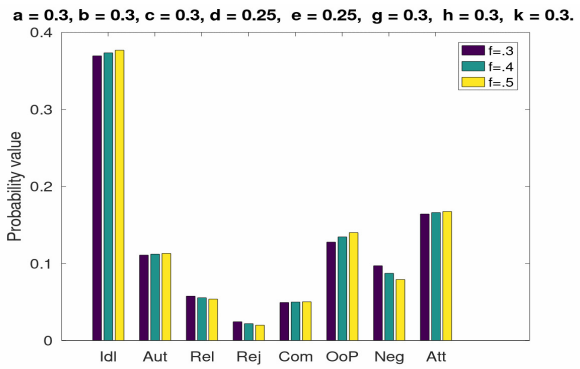
(c)



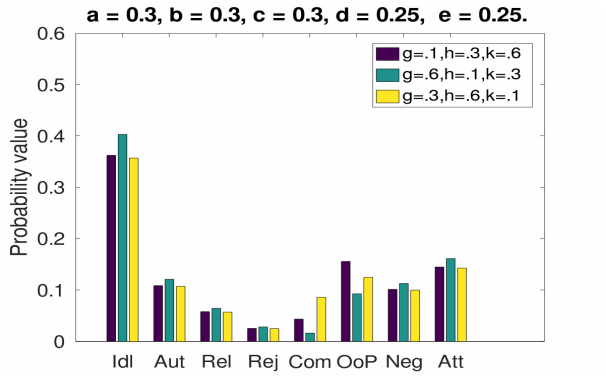
(d)



(e)



(f)



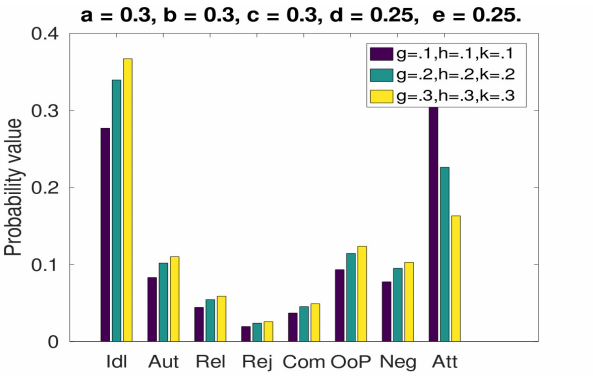
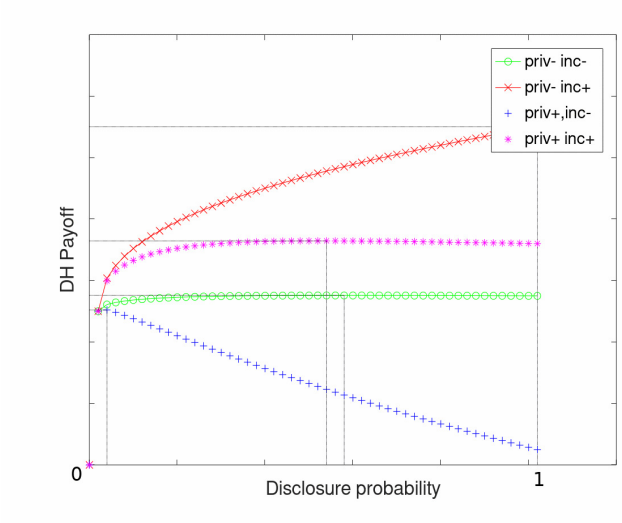


Figure 6. Payoff variation in function of discolure probability for varying privacy concession and incentive motivation



C. Equilibrium solution

Each player tries to maximize his/her profit (utility or payoff) function by choosing an appropriate strategy with knowledge of the strategy space and profit functions of the other players but with no information concerning the current strategy used by rivals. Therefore, each player must conjecture the strategy(ies) used by his/her rival(s).

In stochastic games, the number of players and possible states are finite, then it must have an equilibrium solution [22]. Moreover, the existence of the NE for the proposed game model results from the fact that the objective function defined in the previous subsection is continuous and defined on a compact [13]. We solve the game equilibrium numerically by solving the following optimization problem:

$$p_f := \text{Argmax}\ \{U(p)\,;\, p \in [0,1]\}\,, \tag{1}$$

p_f is the optimal probability of disclosing private data. For simplicity and without loss of generality, we use normalized values of privacy concession and incentive motivation to highlight the influence of these parameters on decision making by DH. Figure 6 presents normalized values of DH payoff in function of disclosure probability for varying incentive motivation and privacy concession. For high privacy concession, disclosure probability and DH payoff are low due to the compromise between privacy preservation and incentive motivation. For low privacy concession, disclosure probability is close to 1 and DH payoff is high, decision is quite evident when data are not sensitive.

VI. Conclusion

In this work, we discussed security concerns in a weight loss program context of e-health application. The dynamic nature of new environments such as IoT, M2M and Web leads to new challenges in relation with data privacy. To model the behavior of involved actors, we propose a game model for privacy preservation based on Markovian process. Depending on the adversary actions, each player has to choose among a set of strategies to switch to a new state. Each player aims to maximize his/her payoff by the end of the game. Then, we validate our theoretical findings through simulation results. In the future, many directions can be explored. First, we will focus on privacy and incentive parameters changes and their impact on players behaviors. Second, we will study the 'long term' players payoffs and their effect on the game events. Third, we can change the actor types in the weight loss program scenario and study the new actions and payoffs models.

References

[1] F. G. on M2M Service Layer, "M2m enabled ecosystems ehealth," ITU-T, Focus Group Technical Report, 04 2014.

[2] D. Lake, R. Milito, M. Morrow, and R. Vargheese, "Internet of things: Architectural framework for ehealth security," *Journal of ICT Standardization*, vol. 34, pp. 301–328, January 2014.

[3] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118 – 137, 2018.

[4] ETSI, "ehealth; standardization use cases for ehealth," European Telecommunications Standards Institute, Tech. Rep. ETSI TR 103 477 V1.2.1, August 2020.

[5] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "Iot privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[6] A. Riahi Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in iot-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[7] G. Zhu, H. Liu, and M. Feng, "An evolutionary game-theoretic approach for assessing privacy protection in mhealth systems," *International Journal of Environmental Research and Public Health*, vol. 15, no. 10, p. 2196, Oct 2018. [Online]. Available: http://dx.doi.org/10.3390/ijerph15102196

[8] A. Meharouech, J. Elias, S. Paris, and A. Mehaoua, "A game theoretical approach for interference mitigation in body-to-body networks." in *ICC Workshops*. IEEE, 2015, pp. 259–264.

[9] C. Yi, Z. Zhao, J. Cai, R. L. de Faria, and G. M. Zhang, "Priority-aware pricing-based capacity sharing scheme for beyond-wireless body area networks," *Computer Networks*, vol. 98, pp. 29 – 43, 2016.

[10] N. Kumar, K. Kaur, A. Jindal, and J. J. Rodrigues, "Providing healthcare services on-the-fly using multi-player cooperation game theory in internet of vehicles (iov) environment," *Digital Communications and Networks*, vol. 1, no. 3, pp. 191 – 203, 2015.

[11] M. Pasha and S. Shah, "Framework for e-health systems in iot-based environments," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–11, 06 2018.

[12] D. Lin, Y. Tang, F. Labeau, Y. Yao, M. Imran, and A. V. Vasilakos, "Internet of vehicles for e-health applications: A potential game for optimal network capacity," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1888–1896, 2017. [Online]. Available: https://doi.org/10.1109/JSYST.2015.2441720

[13] M. Hamdi and H. Abie, "Game-based adaptive security in the internet of things for ehealth," in *IEEE International Conference on Communications (ICC)*, Sydney, Australia, June 2014, pp. 920–925.

[14] I. T. U. T. S. Sector, *Series H: Audiovisual and Multimedia Systems : E-health Multimedia Services and Applications – Interoperability Compliance Testing of Personal Health Systems (HRN, PAN, LAN and WAN) : Conformance of ITU-T*

H.810 Personal Health Devices : PAN/LAN/TAN Interface Part 1: Optimized Exchange Protocol : Agent. ITU-T, 2015.

[15] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. de Montjoye, and A. Bourka, "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics," *CoRR*, vol. abs/1512.06000, 2015.

[16] T. Kanwal, A. Anjum, and A. Khan, "Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities," *Cluster Computing*, 04 2020.

[17] M. Halkidi and I. Koutsopoulos, "A game theoretic framework for data privacy preservation in recommender systems," in *Proceedings of the 2011 European Conference on Machine Learning and Knowledge Discovery in Databases - Volume Part I*, ser. ECML PKDD'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 629–644.

[18] F. Wartena, J. Muskens, L. Schmitt, and M. Petkovic, "Continua: The reference architecture of a personal telehealth ecosystem," in *The 12th IEEE International Conference on e-Health Networking, Applications and Services*, July 2010, pp. 1–6.

[19] R. Karimi Adl, M. Askari, K. Barker, and R. Safavi-Naini, "Privacy consensus in anonymization systems via game theory," in *Data and Applications Security and Privacy XXVI*, N. Cuppens-Boulahia, F. Cuppens, and J. Garcia-Alfaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 74–89.

[20] L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? a contract theoretic approach." *J. Sel. Topics Signal Processing*, vol. 9, no. 7, pp. 1256–1269, 2015.

[21] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Transactions on Big Data*, vol. abs/1512.00327, 2017.

[22] X. Liang and Z. Yan, "A survey on game theoretical methods in human-machine networks," *Future Generation Computer Systems*, 2017.