Every Anonymization Begins with k: A Game-Theoretic Approach for Optimized k Selection in k-Anonymization

Anuraag Kotra, AbdelRahman Eldosouky, and Shamik Sengupta
Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA
Emails: akotra@nevada.unr.edu, iv727@vt.edu, ssengupta@unr.edu

***Abstract*—Privacy preservation is one of the greatest concerns when data is shared between different organizations. On the one hand, releasing data for research purposes is inevitable. On the other hand, sharing this data can jeopardize users' privacy. An effective solution, for the sharing organizations, is to use anonymization techniques to hide the users' sensitive information. One of the most popular anonymization techniques is k-Anonymization in which any data record is indistinguishable from at least k-1 other records. However, one of the fundamental challenges in choosing the value of k is the trade-off between achieving a higher privacy and the information loss associated with the anonymization. In this paper, the problem of choosing the optimal anonymization level for k-anonymization, under possible attacks, is studied when multiple organizations share their data to a common platform. In particular, two common types of attacks are considered that can target the k-anonymization technique. To this end, a novel game-theoretic framework is proposed to model the interactions between the sharing organizations and the attacker. The problem is formulated as a static game and its different Nash equilibria solutions are analytically derived. Simulation results show that the proposed framework can significantly improve the utility of the sharing organizations through optimizing the choice of k value.**

I. INTRODUCTION

In the big data era, vast amounts of data are constantly being generated, collected, and analyzed because of the ease of generating and distributing data in its digital formats. Companies and organizations use the accumulated data to personalize their services, optimize their decision making, and to predict future trends of the users [1]. However, these practices raise many public concerns about the users' privacy especially as this data contains many personal and sensitive information. In response, organizations usually deploy powerful security mechanisms to protect the stored data against different cyber attacks [2]. Similarly, encryption-based security systems were shown to be effective when data is shared between different locations of the same organization, e.g., patients' remote monitoring [3].

However, as organizations often need to share or publish the stored data, e.g., sharing electronic health records between different organizations, traditional security mechanisms cannot be used to protect the users' privacy as they are applied locally. This shortcoming was the main enabler for using data anonymization techniques to hide the sensitive information within a dataset. For instance, information such as the name, address, and phone number can be removed before sharing the data. However, it was shown that the remaining data, after removing the sensitive information, can still be used to identify the users by figuring out the unique characteristics in this data [4]. Therefore, more effective anonymization techniques have been proposed in literature to preserve the privacy while withstanding possible attacks. The key idea behind such techniques is to ensure that the records of the shared datasets are indistinguishable. This can be achieved by removing some information from the dataset to decrease the probability of identifying individual records. Examples of such techniques include k-anonymization [5], l-diversity [6], and t-closeness [7]. For instance, in k-anonymization the dataset is anonymized such that each record is indistinguishable from at least $k-1$ other records [5]. Both l-diversity and t-closeness are extensions to k-anonymization which make more changes to the dataset in order to make it harder to differentiate the records and the attributes.

However, even such models were shown to be prone to specific attacks such as background knowledge attack [8], in which the attacker uses background knowledge such as demographic information and public records to increase its probability of identifying the records. Since, such types of attacks affect k-anonymization, l-diversity, and t-closeness, and that k-anonymization is the basic technique behind l-diversity, and t-closeness, this work will mainly focus on k-anonymization. Another popular type of attacks that affects k-anonymization, is the homogeneity attack [9] in which the attacker can reveal the private information when all the values of sensitive attributes are the same in one equivalence class.

One way to increase the privacy achieved by k-anonymization is to increase the value of k as this implies the need for differentiating each record from a bigger number of records. However, increasing the value of k will increase the information loss, i.e., more information will be removed from the data. This, in turn, will reduce the value of the shared information, when received by other organizations. Therefore, the organizations need to carefully choose the value of k to maximize the privacy while minimizing information loss, which represents a real challenge. In [10], the authors proposed two algorithms to reduce the information loss associated with using k-anonymization. However, these algorithms depend on the structure of the data and cannot be generalized. To this end, choosing the optimal value of k, in k-anonymization, remains an open problem in privacy preserving.

In this work, we propose a game-theoretic model to determine the value of k, in k-anonymization. Game theory is a powerful mathematical framework that enables to study the interactions between parties with opposing goals [11]. The key idea, here, is that each organization will choose the

This research is supported by the National Science Foundation (NSF), USA, Award #1739032.

value of k that maximizes its outcome based on the expected attacks. Meanwhile, attackers can choose between different types of attacks based on their expected outcomes, when an organization chooses a specific k. While game theory has been used, in literature, to study the privacy [12] and [13], such works do not apply to data anonymization and, hence, the problem of finding k requires its own analysis.

The main contribution of this paper is to develop a novel game-theoretic framework that allows the organizations to determine the optimal value of k, in k-anonymization. In particular, we consider a scenario in which more than one organization share their data to a common platform. Each organization gets a reward from the common platform based on the level of anonymization, i.e., a higher level of anonymization will increase the information loss, and, hence, decrease the reward. The framework considers two types of de-anonymization attacks which are background knowledge and homogeneity attack. We formulate the problem as a static non-zero-sum game in which the organizations are considered as defenders that seek to optimize the choice of k, and an attacker that optimizes the selection of its attack, based on the choice of k. For the formulated problem, we analyze the different cases of achieving a Nash equilibrium by considering both the cases in which pure equilibrium is possible, and the general case of mixed-strategy Nash equilibrium. Simulation results show that the proposed approach can enable the organizations to determine their optimal k value in face of the expected attacks.

The rest of the paper is organized as follows. Section II provides the game formulation and defines the defender's and attacker's utilities. In Section III, the equilibrium analysis is derived for the formulated game. Simulation results are discussed in Section IV. Finally, conclusions are drawn in Section V.

II. Game Formulation

A. Players

Organizations: We consider a scenario in which a group of organizations share anonymized datasets with a common platform, a data collector. All organizations are assumed to use $k-$anonymization technique to make their shared data anonymous. The goal of organization i is to choose the best value of k_i to maximize its payoff, given other organizations k values and the possible attacks on the data. Let $\mathcal{D}$ be the set of all organizations' actions.

Attacker: An attacker targets the dataset, at the data collector side, in order to reveal the private information. We assume the attacker can anticipate the level of anonymization used, by analyzing the structure of the dataset. The attacker has three actions to choose from. Let $a \in \mathcal{A} = \{B, H, N\}$ represents the attacker's possible actions which can be B, performing *background knowledge* attack, H performing *homogeneity attack*, or N, no-attack.

B. Payoffs

Each player wants to maximize its outcome (payoff function) based on its action and other players' actions. Each player's payoff is given by its utility function which defines its outcome in light of the combined actions of all the players.

Organizations: The utility of each organization is given as a function in the reward it gets from the data collector, $r_i(k_i)$, the cost for applying the anonymization technique, $c_i(k_i)$, the probability of data breach, $b_i(k_i, k_{-i}, a)$, and the trust factor $T(k_i)$, where k_{-i} refers to the other organizations' actions. Let u_i be the utility of organization i, it can then be given by:

$$u_i(k_i, k_{-i}, a) = r_i(k_i) \cdot (1 - b_i(k_i, k_{-i}, a)) - c_i(k_i) + T(k_i), \tag{1}$$

where the first term represents the probability of receiving the reward based on all the players' actions.

Next, we discuss, in details, each term in (1). First, the reward function $r_i(k_i)$ is defined as a declining function in k_i such that when the level of anonymization increases, the data collector will give less reward to the organization as the data will be less informative. We propose to define $r_i(k_i)$ as:

$$r_i(k_i) = \frac{1}{k_i} R_i, \tag{2}$$

where R_i is the value of the information at organization i. By using (2), when $k_i = 1$, i.e., no anonymization, the organization can obtain the full value of the reward as $r_i(1) = R_i$. For every $k_i > 1$, the reward will be declining such that, for large values of k_i, e.g., $k_i > 10$, any increase in k_i will cause small decrease in r_i. This can be interpreted as when the anonymization level increases, the information will be less useful up to some point where the increased k_i will have a small effect on the information loss (reward). This can be captured by the heavy tail of the function in (2).

Next, we study effect of choosing k_i on the cost function $c_i(k_i)$. We propose to define the cost as a function in the computational cost, for each organization, as it executes the k-anonymization procedure. The computational cost was shown in [14] to depend on the nature of the data under consideration and was proven to be:

$$O(nm + 2^{t_{\text{in}} \cdot t_{\text{out}}}(t_{\text{in}}.t_{\text{out}}.m + (t_{\text{in}}+t_{\text{out}})\Delta \log(t_{\text{in}}+t_{\text{out}})(t_{\text{in}}.t_{\text{out}}+(t_{\text{in}}+t_{\text{out}}) \log(t_{\text{in}}+t_{\text{out}})))),$$

where n denotes the total number of rows, m is the total number of columns, t_{in} is the number of different input row types, t_{out} is the number of different output row types such that $t_{\text{in}}/t_{\text{out}} = k$.

Here, we use this time complexity to represent the cost associated with k-anonymization in (1) as follows:

$$c_i(k) = \beta\Big(n.m + 2^{t_{\text{in}} \cdot t_{\text{out}}}\Big(t_{\text{in}}.t_{\text{out}}.m + (t_{\text{in}} + t_{\text{out}}).\log(t_{\text{in}} + t_{\text{out}})(t_{\text{in}}.t_{\text{out}} + (t_{\text{in}} + t_{\text{out}}) \log(t_{\text{in}} + t_{\text{out}}))\Big)\Big),$$

where β is a conversion factor from the time complexity to its equivalent monetary value.

Next, the trust factor is defined as how much each organization can trust the common platform (the data collector) to secure the data. This trust factor is chosen to depend on the value of k_i such that $T(k_i) = \gamma \cdot k_i$, where, γ is the *co-efficient of trust*.

Finally, we consider the breach probability for each organization's shared data, $b_i(k_i, k_{-i}, a)$. In [15], it was shown that the information breach probability can be given by:

$$b(a, k_i) = \frac{p(a)}{\alpha k_i + 1}, \tag{3}$$

Where, $p(a)$ is probability of a successful attack, based on the attack type, and $\alpha > 0$ is a measure of information security. Note that, in [15], the probability of breach is given as a function in the organization's investment. Here, we assume that k_i represents the organization's investment in protecting the privacy of its shared data.

Equation (3) represents the organization's own probability of breach. In case of multiple organizations sharing to the same platform, this probability will increase as an attacker can link information from different datasets to identify the records [16]. Here, we propose to model this interdependency similar to [17] such that the interdependent probability between two organizations is given as:

$$b(a, k_i, k_{-i}) = 1 - (1 - \frac{p(a)}{\alpha k_i + 1})(1 - \frac{p(a)}{\alpha k_{-i} + 1}). \tag{4}$$

Substituting (4) in (1), the utility of any organization can then be given as:

$$\begin{aligned} u_i(k_i, k_{-i}, a) = \frac{R_i}{k_i} \cdot (1 - \frac{p(a)}{\alpha k_i + 1}) \\ \cdot (1 - \frac{p(a)}{\alpha k_{-i} + 1}) - c_i(k_i) + \gamma \cdot k_i. \end{aligned} \tag{5}$$

Attacker: For the case of two organizations, the attacker's utility can be given in terms of its probability of achieving the reward from the information and the cost to apply its attack. Thus, we define the attacker's utility u_a as follows:

$$u_a(k_1, k_2, a) = b(a, k1, k_2)R_a - c_a(a), \tag{6}$$

where R_a is the reward for revealing the real data that can be achieved based on the combined breach probabilities of the datasets and $c_a(a)$ is the cost of performing each type of the attack.

Note that (4) can be rewritten as:

$$b(a, k_1, k_2) = \frac{p(a)}{(\alpha k_1 + 1)} + \frac{p(a)}{(\alpha k_2 + 1)} - \frac{p(a)}{(\alpha k_1 + 1)} \frac{p(a)}{(\alpha k_2 + 1)}, \tag{7}$$

and, thus, the attacker's utility in (6) can be given as:

$$\begin{aligned} u_a(k_1, k_2, a) = \Big(\frac{p(a)}{(\alpha k_1 + 1)} + \frac{p(a)}{(\alpha k_2 + 1)} \\ - \frac{p(a)}{(\alpha k_1 + 1)} \frac{p(a)}{(\alpha k_2 + 1)} \Big) R_a - c_a(a), \end{aligned} \tag{8}$$

Here, according to the nature of homogeneity attack, the attacker will benefit if the two organizations are using the same anonymization level. This is because of the similar structure of the shared data. In this case, the probability of a successful attack will be higher. Let $p(H_s)$ be the success probability of the homogeneity attack when the organizations use the same anonymization level. Similarly, let $p(H_d)$ be the success probability of the homogeneity attack when the organizations use different anonymization levels, such that $p(H_s) > p(H_d)$. We assume $p(B) > p(H_d) > 0$, i.e., the success probability of background attack is higher than that of the homogeneity attack with different anonymization levels, that is because the attacker can link between the shared data and have extra information (background knowledge). However, $p(B)$ can be higher or lower than $p(H_s)$.

The cost of performing the background knowledge attack is assumed to be higher than that of the homogeneity attack, i.e., $c_a(B) > c_a(H) > 0$. This is because the attacker will spend more time collecting the background information and linking the similar information. Note that, when the attacker chooses not to attack, its utility $u_a(N, k_1, k_2)$ will equal zero. This choice will be superior to the attacker if the cost of performing the attack exceeds the reward from revealing the information.

After considering the success probabilities of the different attack types, we reconsider the organizations' utilities in (5). We notice that each organization can obtain a fraction of the reward R_i that depends on the attack's success probability. Let $\delta = \frac{1}{k_i} \cdot (1 - \frac{p_{\max}(a)}{\alpha k_i + 1}) \cdot (1 - \frac{p_{\max}(a)}{\alpha k_{-i} + 1})$ be the minimum fraction of R_i that an organization can achieve based on the maximum success probability of the available attacks, i.e., $p_{\max}(a)$. We refer to δR_i as the minimum profit factor.

To this end, we define a game $\mathcal{G}$= $\{\mathcal{N}, \mathcal{D}, \mathcal{A}, \mathcal{U}\}$ such that $\mathcal{N}$ is the set of the players which include all the organizations as well as the attacker and $\mathcal{U}$ is the set of the all players' utilities. The goal of each player is to take actions to maximize its utility given the actions of other players. When no player can improve its utility by unilaterally changing its actions, the game is said to be at equilibrium. The notion of equilibrium, in game theory, is referred to as Nash equilibrium [18]. Nash equilibrium can either be pure Nash equilibrium, or mixed-strategy Nash equilibrium. A pure strategy equilibrium, is when every player has only one action/ strategy at equilibrium. On the other hand, a mixed Nash equilibrium represents a probability distribution over each player's set of available actions [19]. Next, we study the possible cases of equilibrium, both pure and mixed strategies for the proposed game.

III. Proposed Game Solution

The studied game is a finite static non-zero-sum game which is known to have a Nash equilibrium, either pure or mixed-strategy. For the sake of analytical tractability, we consider the case where each organization can choose between two k values, i.e., k_L and k_H. These values represent choosing low and high values for k, respectively. Based on these values, each organization will have two minimum profit factors δ_H and δ_L corresponding to the choice of k_L and k_H, respectively.

Let p_1 be the probability of the first organization to choose k_L such that it chooses k_H with probability $1 - p_1$. Similarly, the second organization can choose k_L and k_H with probabilities p_2 and $1 - p_2$, respectively. The attacker, on the other hand, will have a probability distribution of q_B, q_H, q_N of choosing the actions B, H, and N, respectively. We start the analysis

by considering the cases in which the game $\mathcal{G}$ can have a pure strategy Nash equilibrium.

Proposition 1. *Let* $k_i^* = \arg\max_{k_i} \frac{R_i}{k_i} - c_i(k_i) + \gamma \cdot k_i$. *Then, the tuple* (k_i^*, k_{-i}^*, N) *constitute a pure strategy Nash equilibrium for* $\mathcal{G}$ *when the attacker is not able to achieve a positive utility.*

Proof. We note that, the attacker's utility for no-attack is zero, i.e., $u_a(k_1, k_2, N) = 0$. The attacker can only turn to this choice if all the other actions yield a negative utility, i.e., all the utility instances for choosing B and N with the different combinations of k_L and k_H, for each organization, will be result in a negative attacker's utility. Therefore, choosing the action N will be a dominant strategy for the attacker. In this case, each organization's utility will be:

$$u_i(k_i, k_{-i}, N) = \frac{R_i}{k_i} - c_i(k_i) + \gamma \cdot k_i, \tag{9}$$

which clearly depends only on the organization's action and not on the other players' actions. In this case, each organization will chose the value of k that maximizes its utility in (9). Hence, $k_i^* = \arg\max_{k_i} \frac{R_i}{k_i} - c_i(k_i) + \gamma \cdot k_i$, it will represent the optimal organization's choice under no-attack scenario. In this case, no player will have an incentive to change its choice and, therefore, the actions tuple (k_i^*, k_{-i}^*, N) is a pure strategy Nash equilibrium for the game. □

From Proposition 1, the attacker's probability q_N of choosing the action N will be either 1 or 0 based on whether the action N dominates the other actions or it is being dominated by another action. Therefore, we will consider only two actions for the attacker, i.e., B and H which can be selected by the probabilities q and $1-q$, respectively when $q_N = 0$. Similarly, for the organizations, we note the similarity in their actions and utilities, thus, they will have the same equilibrium profile which can be given by p for selecting k_L and $1-p$ for selecting k_H.

Similar to the attacker, each organization can have a dominant strategy under some circumstances and, hence, the probability p can be either 0 or 1 based on the dominant strategy. This is shown in the next proposition.

Proposition 2. *Each organization will have a dominant strategy when the value of* R_i *is large enough such that the minimum profit factor is the dominant term in the organization's utility, i.e.,* $\delta_H R_i > \gamma \cdot k_H - c_i(k_H)$ *and* $\delta_L R_i > \gamma \cdot k_L - c_i(k_L)$. *The dominant strategy can then be given as the solution of:*

$$k_i^* = \arg\max_i \delta_i R_i - c_i(k_i) + \gamma \cdot k_i, \quad i \in \{L, H\}$$

Proof. The values of $\delta_H R_i$ and $\delta_H R_i$ represent the minimum fractions of the reward each organization can achieve, under the attacker's maximum probability of success. When the values of R_i are large enough to make these minimum profit factors higher than the rest of the utilities, each organization can expect that any other attacker's action will not lower its utility. Thus, the organization can determine its dominant strategy while neglecting the attacker's effect. □

Note in Proposition 2, a high reward can eliminate the attacker's effect, however, determining the optimal k value depends on the other factors of the utility.

To this end, when no player has a dominant strategy, the players will need to consider the mixed-strategy Nash equilibrium in order to determine the probability of choosing each action. These mixed strategies can be calculated when the players are indifferent between choosing their actions, i.e., the expected utility of choosing each action will be the same. For instance, the organizations can choose their p such that the attacker's expected utility from choosing the action B will equal to that of choosing the action H. The attacker's expected utility from choosing the action B can be given by:

$$\begin{aligned}\mathbb{E}(u_a(k_1, k_2, B)) = {} & p \cdot p \cdot u_a(k_L, k_L, B) + p \cdot (1-p) \cdot \\ & u_a(k_L, k_H, B) + (1-p) \cdot p \cdot \\ & u_a(k_H, k_L, B) + (1-p) \cdot (1-p) \cdot \\ & u_a(k_H, k_H, B).\end{aligned} \tag{10}$$

The expected utility of choosing the action H can be written in a similar way to (10). For the attacker to be indifferent between its actions, its expected utility for choosing B must equal that of choosing H. Solving both equations together, an organization's probability of choosing k_L, i.e., p can then be given as the solution of the quadratic equation:

$$\begin{aligned}&\Big(\frac{2p^2(B) - 2p^2(H_d)}{(\alpha k_L + 1)(\alpha k_H + 1)} - \frac{p^2(B) - p^2(H_s)}{(\alpha k_L + 1)^2} - \frac{p^2(B) - p^2(H_s)}{(\alpha k_H + 1)^2}\Big) \cdot R_a \\ &\cdot p^2 + \Big(\frac{p(B) - p(H_d)}{(\alpha k_L + 1)} - \frac{p^2(B) - p^2(H_d)}{(\alpha k_L + 1)(\alpha k_H + 1)} + \frac{p^2(B) - p^2(H_s)}{(\alpha k_H + 1)^2} \\ &- \frac{p(B) - 2 \cdot p(H_s) + p(H_d)}{(\alpha k_H + 1)}\Big) 2 \cdot R_a \cdot p + \Big(\frac{2p(B) - 2p(H_s)}{(\alpha k_H + 1)} \\ &- \frac{p^2(B) - p^2(H_s)}{(\alpha k_H + 1)^2}\Big) R_a - c_a(B) + c_a(H) = 0.\end{aligned} \tag{11}$$

Note that, only one solution to (11) will represent a valid probability, and the other solution will be rejected. After calculating the probability p, the attacker's probability q can be calculated in a similar way by considering the expected utility of one of the organizations. Note that, due to the symmetry between the organizations, considering the utilities of both organizations will be redundant. For an organization to be indifferent between its actions, its expected utilities must be the same for both of its actions. Therefore, the attacker can choose the probability q by solving the equation:

$$\begin{aligned}q = {} & \Big(u_1(k_H, k_H, H) - u_1(k_L, k_H, H) + p\Big(u_1(k_H, k_L, H) \\ & - u_1(k_H, k_H, H) - u_1(k_L, k_L, H) + u_1(k_L, k_H, H)\Big)\Big) \Big/ \\ & \Big(u_1(k_L, k_H, B) - u_1(k_L, k_H, H) - u_1(k_H, k_H, B) + u_1(k_H, \\ & k_H, H) + p\Big(u_1(k_L, k_L, B) - u_1(k_L, k_L, H) - u_1(k_L, k_H, B) + \\ & u_1(k_L, k_H, H) - u_1(k_H, k_L, H) + u_1(k_H, k_H, B) + u_1(k_H, \\ & k_L, H) - u_1(k_H, k_H, H)\Big)\Big)\end{aligned} \tag{12}$$

Given the value of p from (11), the value of q can be uniquely computed from (12). The mixed strategy equilibrium

can then be given as $(p, 1-p)$ for the organizations and $(q, 1-q)$ for the attacker. Note, in this section, the solution of a single stage game was introduced. In future work, we will consider a dynamic game, i.e., a game that changes over time, e.g., [20], in which the players' trust evolve over time.

IV. Simulation Results And Analysis

For our simulations, we set the value of $k_L = 4$ and $k_H = 7$ such that k_H is slightly higher than k_L to better highlight the effect of these values on the utilities. Other system parameters are set to $\alpha = 1$, $\gamma = 0.6$, and $\beta = 10^{-6}$. The success probabilities of the different attacks are assumed to be $P(H_d) = 0.3$, $P(H_s) = 0.7$, and $P(B) = 0.6$. We assume similar dataset structures between the organizations, so that, the cost function is only affected by the choice of k.

First, we solve the formulated game $\mathcal{G}$ using the analysis in Section III. We allow the values of the reward R to change from 16 to 25. These values represent the monetary rewards the data collector will give to the organizations as a reward for sharing the data. Here, we use abstract values, however, in a real-life scenario, the data collector needs to estimate these values to be proportional to the cost. The equilibrium strategies for both the attacker and defender are shown in Tables I and II, respectively. We note that, when the values of R are less than 17, the attacker cannot achieve a positive utility, and, hence, it will choose not to attack. This situation corresponds to the case of Proposition 1 and the defender's utility is calculated using (9). In this case, the defender will have a pure strategy of choosing k_H. For the values of R between 18 and 21, both the attacker and the defender will have mixed strategies, i.e., choosing their actions with certain probabilities. Finally, for large values of R, the attacker will benefit only if it performed the background knowledge attack, in this case the defender can choose between the two values of k with k_H being superior, i.e., it has a higher probability to be chosen.

Fig. 1 shows the expected utilities calculated using the equilibrium strategies in Tables I and II. These utilities are compared to the case where one player chooses random probabilities while the other plays its equilibrium strategy. From Fig. 1, we can see that when a player deviates from the equilibrium strategy, to a random strategy, it cannot achieve a higher utility. This corroborates the importance of studying Nash equilibrium as it represents the best each player can do given their opponent's actions. We can also see from Fig. 1 that the players' utilities do not exhibit a monotonic increase in R as the utility depends on the players' actions.

In Fig. 2, we show the effect of the success probability of the background knowledge attack, i.e., $p(B)$ on the equilibrium strategies of the players. Note that, the values of $p(B)$ are chosen to start at 0.4 to satisfy the assumption $p(B) > p(H_d)$. The equilibrium strategies in Fig. 2 are calculated in a similar way to the values in Tables I and II. The simulation parameters are the same as Fig. 1 and the value of R is fixed to 19. This value was chosen as the attacker has almost equal probability of choosing its actions under this value. From Fig. 2, we can see that when $p(B)$ is slightly higher than $p(H_d)$ i.e.,

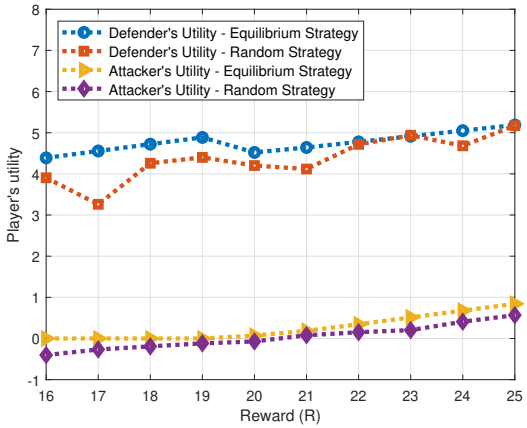

Fig. 1. The defender's and the attacker's utilities at equilibrium at different reward R values.

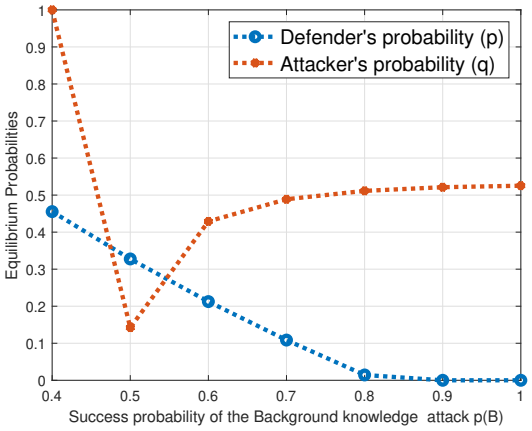

Fig. 2. The defender's and the attacker's equilibrium probabilities at different success probabilities for background knowledge attack $p(B)$ values.

$p(B) = 0.4$ the attacker will have a high value of q which corresponds to the probability of choosing the background knowledge attack. At the same point, the defender will be choosing k_H with slightly higher probability. However, as the value of $p(B)$ increases, the defender will prefer to use k_H more which lowers the attacker's utility and force it to switch to the homogeneity attack because of its lower cost. This can be seen as the value of q decreases when $p(B) = 0.5$. As $p(B)$ increases more, it will become closer to $p(H_s)$ and in this case, the defender will stick more to choosing k_H as it achieves more trust in protecting the data. Meanwhile, the attacker will choose the background knowledge attack with slightly higher probability.

In Fig. 3, we study the effect of the success probability of the homogeneity attack, for similar values of k, i.e., $p(H_s)$ on the equilibrium strategies of the players. Similar to Fig. 2, the values of $p(H_s)$ are starting at 0.4 so that $p(H_s) > p(H_d)$. The simulation parameters are the same as Fig. 2 and $p(B) = 0.6$. From Fig. 3, we can see that when $p(H_s)$ is less than $p_(B)$ i.e., $p(H_s) < 0.6$, the attacker will have a higher probability of choosing the background knowledge attack. This probability will decrease as $p(H_s)$ is equal to $p(B)$ or higher.

TABLE I
ATTACKER'S EQUILIBRIUM STRATEGIES

R	16	17	18	19	20	21	22	23	24	25
B	0	0	0.0971	0.4290	0.7175	0.97	1	1	1	1
H	0	0	0.9029	0.5710	0.2825	0.03	0	0	0	0
N	1	1	0	0	0	0	0	0	0	0

TABLE II
DEFENDER'S EQUILIBRIUM STRATEGIES

R	16	17	18	19	20	21	22	23	24	25
$\mathbf{k_L}$	0	0	0.2187	0.2125	0.2070	0.2019	0.1973	0.1937	0.1893	0.1857
$\mathbf{k_H}$	1	1	0.7813	0.7875	0.7930	0.7981	0.8027	0.8063	0.8107	0.8143

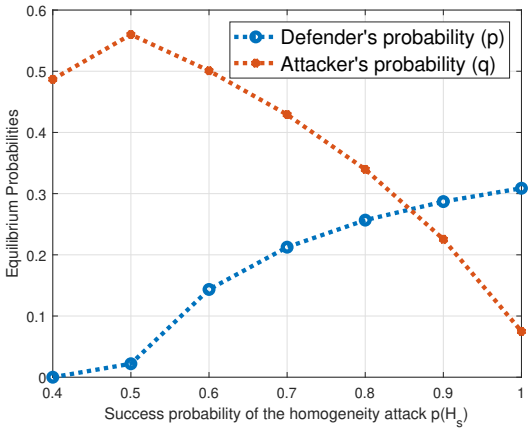

Fig. 3. The defender's and the attacker's equilibrium probabilities at different success probabilities for homogeneity attack $p(H_s)$ values.

In this case, the attacker will prefer to choose the homogeneity attack with higher probability especially with the increase in its success probability. For the same range of probabilities, the defender will choose k_H with higher probability. However, this probability will decrease as $p(H_s)$ increases.

V. CONCLUSIONS

In this paper, we have studied the problem of determining the optimal value of k for the $k-$anonymization technique. We have formulated the problem using a game-theoretic model that involves three players which are an attacker and two organizations sharing data with a common platform, a data collector. In particular, we have considered two common types of attacks that can affect k-anonymization techniques. We have defined the players' utilities resulting from the interactions between the three players. Then, we have provided the mathematical derivation of the different Nash equilibria, for the proposed game. Simulation results have shown that the proposed model can help the organizations to maximize their utilities, under attack, through choosing the optimal k values.

REFERENCES

[1] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[2] S. Badsha, I. Vakilinia, and S. Sengupta, "Privacy preserving cyber threat information sharing and learning for cyber defense," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2019, pp. 0708–0714.

[3] A. Eldosouky and W. Saad, "On the cybersecurity of m-health iot systems with led bitslice implementation," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2018, pp. 1–6.

[4] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[5] L. SWEENEY, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 571–588, 2002. [Online]. Available: https://doi.org/10.1142/S021848850200165X

[6] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," in *22nd International Conference on Data Engineering (ICDE'06)*. IEEE, 2006, pp. 24–24.

[7] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 2007, pp. 106–115.

[8] T. Li, N. Li, and J. Zhang, "Modeling and integrating background knowledge in data anonymization," in *2009 IEEE 25th International Conference on Data Engineering*. IEEE, 2009, pp. 6–17.

[9] Q. Wang, Z. Xu, and S. Qu, "An enhanced k-anonymity model against homogeneity attack." *JSW*, vol. 6, no. 10, pp. 1945–1952, 2011.

[10] Z. Liang and R. Wei, "Efficient k-anonymization for privacy preservation," in *2008 12th International Conference on Computer Supported Cooperative Work in Design*. IEEE, 2008, pp. 737–742.

[11] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge university press, 2012.

[12] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacundefinedar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, Jul. 2013. [Online]. Available: https://doi.org/10.1145/2480741.2480742

[13] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Computing Surveys (CSUR)*, vol. 50, no. 2, pp. 1–37, 2017.

[14] R. Bredereck, A. Nichterlein, R. Niedermeier, and G. Philip, "The effect of homogeneity on the computational complexity of combinatorial data anonymization," vol. 28, no. 1, Jan 2014, pp. 65–91. [Online]. Available: https://doi.org/10.1007/s10618-012-0293-7

[15] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, Nov. 2002. [Online]. Available: http://doi.acm.org/10.1145/581271.581274

[16] A. S. Sattar, J. Li, J. Liu, R. Heatherly, and B. Malin, "A probabilistic approach to mitigate composition attacks on privacy in non-coordinated environments," *Knowledge-based systems*, vol. 67, pp. 361–372, 2014.

[17] H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and it security investment: Impact of interdependence risk." in *WEIS*, 2005.

[18] S. Sengupta, M. Chatterjee, and K. Kwiat, "A game theoretic framework for power control in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 2, pp. 231–242, 2009.

[19] A. Eldosouky, W. Saad, and D. Niyato, "Single controller stochastic games for optimized moving target defense," in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.

[20] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting uavs against gps spoofing," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2840–2854, 2020.