Computers and Electrical Engineering 100 (2022) 107894

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A privacy enhancing model for Internet of Things using three-way decisions and differential privacy☆

Waqas Ali *, Mohammad Nauman, Nouman Azam

National University of Computer and Emerging Sciences, Pakistan

ARTICLE INFO

Keywords:
Data privacy
Differential privacy
Three-way decisions
Internet of Things

ABSTRACT

The recent advancements in Internet of Things (IoT) have brought enormous advantages for businesses. These benefits are achieved by services that collect large volumes of data that is collected for analysis. The data may also contain sensitive information. Privacy of such data is an important research challenge. Differential privacy is a recent technique for data privacy. It works by anonymizing the attributes that may contain sensitive information. An essential step before applying differential privacy is the division of attribute set into three groups called sensitive, non-sensitive and ambiguous. A key issue in existing studies is that the division of attribute set is done manually by a domain expert and is therefore costly. We introduce a three-way approach for differential privacy and a supporting algorithm for this demarcation of attribute sets. Results indicate that the information content and stability of the dataset improves considerably with our approach.

1. Introduction

Internet of things (IoT) has enormous usage potential in smart homes, Industrial IoTs and medical or healthcare IoTs. This requires collection of large amounts of data that may be stored and shared for analysis. The collected data may contain medical, financial or personal information and its leakage may lead to privacy issues. Many privacy related incidents have been reported in the recent past which demand for efficient and effective solutions for data privacy [1]. On the other hand, in IoT smart homes, there is a greater risk of data and identity theft. Data can be used to analyze human activities and may have serious implications such as robberies.

Different anonymization techniques have been used in IoTs to protect sensitive information. The most common approach is hiding all the sensitive attributes. This however, leads to significant loss in utility of the data for useful analysis [2]. Another common approach is to release only aggregate values [3]. A privacy breach can occur with this approach if someone manages to gain enough aggregate values that provide hints about sensitive data of an individual [3]. *Query auditing* is another approach for data privacy [4]. It works by comparing the results of the past queries with the current query to determine whether or not responding to the same query will lead to a privacy breach. It can then deny those queries that lead to a privacy breach. It is however argued that query denials can also lead to information leakage. The approach of *k-anonymity* was introduced in order to address shortcomings of the earlier techniques. It fails in situations where sensitive values in a class lack diversity [5]. l-diversity was a refinement of *k-anonymity* [6]. It works by making sure that each class of values has enough sensitive values and that the values are distributed evenly. It is not able to prevent attribute disclosure which makes it susceptible to inference attacks [7]. The approach of *t-closeness*

☆ This paper is for special section VSI-sss. Reviews were processed by Guest Editor Dr. Sajid Anwar and recommended for publication.

* Corresponding author.
E-mail address: waqas.ali@nu.edu.pk (W. Ali).

https://doi.org/10.1016/j.compeleceng.2022.107894
Received 5 October 2021; Received in revised form 28 February 2022; Accepted 4 March 2022
Available online 29 March 2022

is a refinement of k-anonymity which works by making sure that the distribution of a sensitive attribute in a class is close to the distribution of the sensitive attribute in the overall table. It however is susceptible to re-identification attacks [8].

Differential privacy is a recent and more effective technique and it overcomes many issues associated with the earlier approaches [9]. It has gained significant popularity in the community, as well as the industry due to its strict guarantees for ensuring protection and security of the data [9]. An important step before applying differential privacy is the division of attributes into sensitive, non-sensitive and ambiguous groups. Sensitive attributes are not stored on the cloud since they contain private data, such as names and other unique identifiers. Non-sensitive attributes do not contain any private data and are therefore stored on the cloud. Ambiguous attributes may contain sensitive data but it may not be used to directly reveal one's private information. We typically want to store these attributes as they contain data that is useful for analysis, such as being used in research or in market analysis for public interest. This division of attributes is typically a tedious, manual process and requires a domain expert which may be time consuming and costly in cases of large datasets. Automated approaches for effective three-way attribute division is of exigent need in this context. We consider the use of three-way decisions for constructing such an approach.

In this paper, we propose a three-way decisions based approach to differential privacy that automatically determines an effective grouping of the attributes. The approach follows an evaluation based interpretation of three-way decisions and uses an evaluation function and a pair of thresholds to place an attribute into one of the three groups. The configuration of thresholds plays a key role in obtaining grouping of the attributes. To obtain effective grouping of attributes, we introduce an algorithm called Three-way Attribute Division Algorithm for Differential Privacy (3WADD) that automatically determines the thresholds by continuously improving the overall utility level of a dataset from analysis and privacy viewpoints. An architecture of privacy preservation based on differential privacy with automated three-way attribute division is also presented. The results in this paper advocates that the proposed approach can be used as an added mechanism for improving the overall performance of differential privacy in IoT.

The rest of the paper is organized as follows: In Section 2, the background of differential privacy and three-way decisions has been reviewed. Section 3 presents an architecture for privacy preservation using differential privacy. Section 4 presents the model proposed in this paper. In this section we discuss the techniques used to categorize the attributes and anonymize the sensitive data. Section 5 presents the details of the experiments, the evaluation metrics and the results of the experiments. Section 6 discusses the conclusion of this research.

2. Related work

In this section, we introduce the background of our proposed approach, which includes differential privacy and three-way decisions.

2.1. An overview of differential privacy

Differential privacy is a technique that addresses many of the issues associated with the earlier approaches [9]. Considering f as a function corresponding to a certain query on a dataset, and D_o as the original dataset with N rows. The key idea of differential privacy is to add noise to the result of a query using the formula [9],

$$f(D_o) + (Lap(\Delta f/\epsilon)). \tag{1}$$

The Δf is known as the sensitivity of a query which is computed as,

$$\Delta f = \max_{i \in \{1,2,3,\ldots,N\}} \|f(D_o) - f(D_i)\|_1, \tag{2}$$

where D_i is the same dataset as D_o without the ith row. Eq. (1) has two terms. The first term $f(D_o)$ denotes the actual result of applying a query using function f on the dataset D_o. The second term is used to add noise to the result of the query. Generally Laplacian noise is added based on the Laplacian distribution with zero mean and a scale factor of $\Delta f/\epsilon$. The Δf in Eq. (2) computes the maximum of the difference between the result of a query on the original dataset D_o and for all datasets D_i where $i \in \{1, 2, \ldots, N\}$. A high value of sensitivity will mean that removing a row from the original dataset D_o has a greater effect on the result of the query and a low value of sensitivity will mean that removing a row from the original dataset D_o has little effect on the result of the query. For a simple count query, Δf will be one because $f(D_o) - f(D_i)$ will be equal to one for all D_i. This is because the difference between the number of rows in the two datasets D_o and D_i is one. The value of ϵ controls the amount of noise in the dataset. Adding a lot of noise may result in a dataset that is highly secure but may not be very useful for analysis thereby having lesser utility for analysis purposes. Adding lesser noise may result in a dataset that has higher utility for analysis but has lesser security. A suitable value of ϵ provides a balance and tradeoff between the utility and security of the dataset [10].

Existing studies on differential privacy can be roughly categorized into two classes. One class of studies focuses on the determination of ϵ and its impact on the overall security and utility of the dataset. A technique for determining ϵ was considered in [11]. A threshold was introduced that keeps ϵ in limits and small enough to provide high privacy guarantee. This technique was used to anonymize query logs of web searches. The utility of the dataset was computed by introducing the measures of *discounted cumulative gain* and *mean average precision*. They were able to maintain an acceptable level of utility between the original and the anonymized logs. The value of ϵ was determined with the help of a threshold which represented the maximum tolerable value for the probability of identifying an individual in [10]. A strict bound was placed on the information leakage to identify the optimal value of ϵ in [2]. Other relevant studies in the same group includes differential privacy for sensor-cloud systems [12] and differential privacy for blockchain data [13].

The second class of studies deal with the identification of dependencies between records or attributes in a dataset and masking these dependencies. One such study is presented in [14]. In particular, correlations and distribution of attributes were build from the records of the dataset to mask the dependencies in the final publishable dataset. A correlated boundary was used to mask the relation between sensitive and non-sensitive attributes in [15]. Adjacency matrices were constructed to identify the dense regions in [16]. The dense regions are reconstructed using the exponential mechanism of differential privacy to hide the correlation between data. Other relevant studies in the same group include differential privacy under dependent tuples [17] and plausible deniability [18].

2.2. Problem under focus

In all of the cases discussed earlier, differential privacy requires manual division of attributes in a dataset as being sensitive, non-sensitive or ambiguous. Sensitive attributes are not saved on the cloud, non-sensitive attributes are saved verbatim while ambiguous attributes are anonymized by adding noise using differential privacy and then saved. The division of attributes is not always obvious and clear [19]. Typically, the knowledge of domain experts is used to provide the necessary division of attributes. In most of the cases, the job of domain experts is time consuming and overwhelming especially when the datasets are large. Automating the division of attributes is an important issue in this context. This however has not been sufficiently addressed in the existing literature. In this paper, we aim to provide an approach in this regards based on the principles of three-way decisions.

2.3. Three-way decisions

Three-way decisions is a new decision making paradigm which provides a human problem solving strategy that aims at representing, understanding and processing the whole in terms of three related parts. Since its inception, the theory has been widely used in many fields and has led to research areas such as three-way clustering [20], three-way classification [21], three-way attribute reduction and many others [22].

Three-way decisions are typically realized by considering the *framework of trisecting and acting* or more recently *trisecting, acting and outcome* [23]. In trisecting, the whole is divided into three parts or regions which is also sometimes referred to as *tripartition*. The acting phase consists of devising effective and efficient strategies for processing the three parts. Outcome measures the effectiveness of trisecting and acting for achieving certain desirable outputs or outcomes. As an example, consider the case of medical decision making. The trisection will consist of dividing the set of patients into three regions, i.e., those having the disease, those that do not have the disease and those for whom there is insufficient evidence to decide either way. The acting will consist of strategies such as giving treatments to all those having the disease, not giving treatments to those not having the disease and performing further tests on patients in the third category. The outcome will measure the effectiveness of the trisecting or equivalently the tripartitioning and the corresponding strategies.

An *evaluation function* and a pair of thresholds are commonly used to obtain the tripartition of the universe (this is also sometimes referred to as *evaluation based interpretation*). Consider an evaluation function $e(x) : U \longrightarrow L$ and a pair of thresholds (α, β). The evaluation function assigns an evaluation value to each object $x \in U$ from a totally ordered set $(L, \preceq)$. The universe U is partitioned based on e and a threshold pair (α, β) as,

$$\mathrm{POS}_{(\alpha,\beta)} = \{x \in U \mid e(x) \succeq \alpha\}, \tag{3}$$

$$\mathrm{NEG}_{(\alpha,\beta)} = \{x \in U \mid e(x) \preceq \beta\}, \tag{4}$$

$$\mathrm{BND}_{(\alpha,\beta)} = \{x \in U \mid \beta \prec e(x) \prec \alpha\}. \tag{5}$$

The three regions provide realization of three-way decisions. In this research, we aim at an approach for automatic division of attributes using three-way decisions into sensitive, non-sensitive and ambiguous attributes. In Section 4, we explain and introduce such an approach.

3. An architecture of privacy preservation with three-way attribute division

To incorporate three-way division of attributes in the automated process of ensuring privacy of data in Internet of things, we present an architecture for privacy preservation using differential privacy. The architecture is shown in Fig. 1. The architecture comprises of two main parts namely *three-way division of attributes* and *privacy of ambiguous attributes*.

The first part, i.e., three-way division of attributes iteratively decides on the a suitable three-way division of attributes which is returned by the *three-way attribute divider* component. It iteratively combines the non-sensitive and ambiguous attributes to form a dataset. The usefulness of the formed dataset is carried by the component called *dataset evaluation*. It considers the aspects of *utility* of the dataset for analysis as well as the *stability* of the dataset to keep a balance between the number of attributes in the non-sensitive and ambiguous groups. The process continues for each dataset and stops when an acceptable level of the considered aspects is reached. In Section 4, we discuss measures which can be used for reflecting the aspects of utility and stability of a dataset. We now explain the components included in the first part.

Three-way Attribute Divider: This component provides three-way division of attributes and divides the set of attributes into sensitive, non-sensitive and ambiguous. Input to this module is the dataset and its output is a three-way division of attributes.

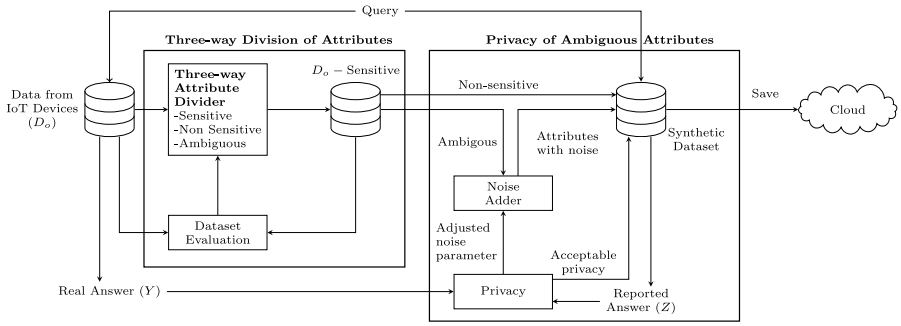

Fig. 1. High level view of the proposed architecture.

An important question is how to obtain the three-way division of attributes. We use three-way decisions based approach in this regards which is explained in the next section.

Dataset Evaluation: This component decides whether a dataset created by the three-way attribute divider is suitable or not. This is achieved by computing different measures reflecting various aspects of dataset usefulness. Inputs to this module is the original dataset (D_o) and the dataset obtained from the three-way divider module (i.e., D_o-Sensitive). The output of this module is a decision on whether a dataset is suitable or not.

The second part of the architecture deals with the privacy of the ambiguous attributes. Once the three-way division of attributes is obtained, the ambiguous attributes need to be protected since they may contain sensitive information. This is done with the help of the noise adder component. In particular, the noise adder component employs the differential privacy mechanism of adding noise to data for anonymization. The amount of noise added to the data depends upon two parameters, one is ϵ and the other is Δf. These parameters are discussed in Section 2.1 and are given in Eqs. (1) and (2). These anonymized attributes are combined with the non-sensitive attributes to form a synthetic dataset. A query is executed on the records of the original dataset and the synthetic dataset. The result of the query on the original dataset and the synthetic dataset are compared to calculate privacy level of the synthetic dataset. If the privacy is lower than a threshold then the noise parameter is adjusted and noise is added to the ambiguous attributes with the new parameter values to obtain another synthetic dataset. This process continues until the privacy is at or above a certain acceptable level. The primary contribution in this research work lies in this first part of the architecture. For the sake of completeness, we also explain the components included in the second part here.

Noise Adder: This component adds noise to the data in the ambiguous attributes based on some parameters using differential privacy mechanism. Input to this module is the data corresponding to ambiguous attributes and the output is the modified data corresponding to ambiguous attributes with noise added to them.

Synthetic Dataset: This component is used to create a synthetic dataset. The synthetic dataset is formed by combining the data corresponding to the ambiguous attributes (with added noise) and the data corresponding to non-sensitive attributes from the original dataset.

Privacy Measure: This module decides whether the synthetic dataset has enough privacy for it to be published. The inputs to this module are the answers of a query on the original and the synthetic datasets which corresponds to the results of $f(D_o)$ and $f(D_i)$ respectively, these are given in Eq. (2). The output of this module is the adjusted noise parameter ϵ if the level of privacy is not acceptable. The level of privacy is denoted by $Lap(\Delta f/\epsilon)$ and is given in Eq. (1).

4. Proposed scheme

In this section, we propose an approach for three-way division of attributes based on three-way decisions. The three-way division of attributes will divide the set of attributes into three pair-wise disjoint groups, namely, *sensitive*, *non-sensitive* and *ambiguous*. Fig. 2 shows the three-way interpretation of attribute division based on the trisecting and acting framework. In the trisecting step, we partition or divide the attributes into three disjoint groups and in the acting step, we take actions of publishing, not publishing and anonymizing the attributes. We aim at an approach that is in contrast to existing approaches. Our model provides an automated three-way division of attributes rather than relying on manual and tedious efforts by domain experts.

4.1. Attribute division using three-way decisions

To obtain the tripartition of the set of attributes or equivalently three-way division of attributes, we consider an evaluation function based three-way decisions discussed in Section 2.3. To define an evaluation function, we consider the data corresponding to an attribute and measures its suitability for providing protection against attacks. In other words, we measure, based on the values of the attributes in the particular dataset, as to how difficult it will be to identify an individual record.

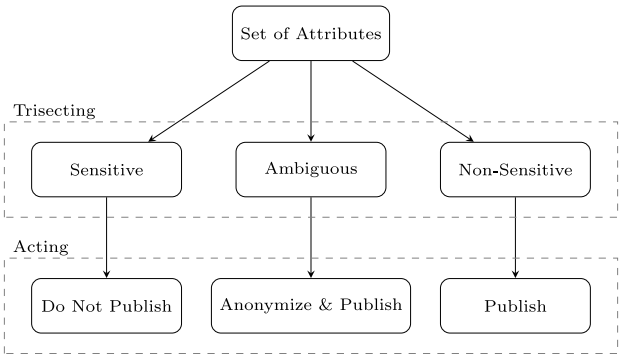

Fig. 2. Three-way decision classification of attributes.

Generally speaking, an attribute with many distinct values may be considered to be less protected compared to an attribute with less distinct values. For instance, consider a dataset corresponding to a hospital containing the attributes of age and disease. Let us assume that all the patients have different age values. In such a case, if an adversary who knows the age of a certain patient can easily identify his/her respective disease from the dataset. In contrast to this, if we assume that all the patients have the same age values, the adversary cannot infer a patient's disease from age because all patients have the same value for this particular attribute. This means that by having higher *information content* in an attribute, i.e., many distinct values for an attribute, we have lesser protection capability in the respective attribute against potential attacks and therefore may be considered as sensitive. On the other hand, if we have lesser information content in an attribute, i.e., very few distinct values for an attribute, we have higher protection capability in the respective attribute against attacks and therefore may be considered as non-sensitive. We employ this measure of information in attributes to construct an evaluation function.

4.1.1. Measures of information content

Entropy is a common measure of computing the amount of information in an attribute [24]. An attribute having high entropy will tend to have high information content and therefore may be considered as sensitive. On the other hand, an attribute having low entropy will tend to have low information content and therefore may be considered as non-sensitive. Finally, for those attributes, whose information content is neither very high nor very low may be considered as ambiguous. The measure of entropy for an attribute A_i belonging to an attribute set At is formally defined as,

$$\text{Entropy}(A_i) = -\sum_{a_i \in A_i} P(a_i) \log P(a_i), \tag{6}$$

where a_i is a particular value of an attribute A_i and $P(a_i)$ is probability with which it occurs. It may be noted that other measures for computing the information content can also be used as evaluation measures. One such measure is the measure of variance. However in the context of information and uncertainty, it has its own strengths and limitations as compared to entropy. For instance, if the distribution of data is discrete and unimodal i.e., the distribution has a single peak, variance is a better measure [24]. However, if the distribution of data is continuous and is bimodal i.e., have multiple peaks, entropy is a better measure. In case of categorical data, variance is completely artificial because one must assign arbitrary numbers to each category and the variance of the data will depend on the assigned numbers which does not reflect the true nature of the data. In such case entropy is a better measure. In this study, we only consider the measure of entropy as evaluation function as our main focus is on the formulation of three-way division of attributes. In future, further evaluation measures may also be explored and incorporated in the proposed approach for fine tunning the results.

4.1.2. Systematic division of attributes

Once the evaluation function values are computed, we next divide the set of attributes into sensitive, non-sensitive and ambiguous groups using the following equations,

$$\text{Sensitive}_{(\alpha,\beta)} = \left\{ A_i \in At \mid e(A_i) \geq \alpha \right\}, \tag{7}$$

$$\text{Non-Sensitive}_{(\alpha,\beta)} = \left\{ A_i \in At \mid e(A_i) \leq \beta \right\}, \tag{8}$$

$$\text{Ambiguous}_{(\alpha,\beta)} = \left\{ A_i \in At \mid \beta < e(A_i) < \alpha \right\}, \tag{9}$$

where the evaluation function $e(A_i)$ is a generalized evaluation function which we realized as a measure of entropy defined in Eq. (6) and (α, β) are the two thresholds used to divide the attributes into three groups. We assume $0 \leq \beta < \alpha \leq 1$ and $\alpha + \beta = 1$ in this paper which ensures that the three sets or groups are disjoints. The attributes whose evaluation function values are at or above threshold α are assigned to the sensitive group while the attributes whose evaluation function values are at or below thresholds β are assigned to the non-sensitive group. The attributes whose evaluation function values are between the two thresholds will be assigned to the

ambiguous group. Next, a dataset is formed by combining the data corresponding to the non-sensitive and ambiguous attributes. Please note that, as mentioned in the previous section, the data corresponding to the ambiguous attributes will be first anonymized using differential privacy before being added to the synthetic dataset.

4.1.3. Utility assessment of resulting datasets

It may be noted that choosing arbitrary threshold values may lead to inefficient division of attributes which may degrade privacy of the data. The selection of proper (α, β) thresholds is an important issue in this context. We consider the computation of effective thresholds as an iterative process where thresholds will be continuously updated by considering the usefulness of the resulting three-way attribute division. Since the three-way division of attributes defines a candidate synthetic dataset, therefore the usefulness of three-way attribute division of attributes is equivalent to the usefulness of the resulting candidate dataset.

We consider two qualitative aspects for assessing the usefulness of a candidate synthetic dataset resulting from a certain three-way attribute division. The first aspect is the information content in the resultant dataset. This aspect is typically quantified in existing studies by making use of the measure of utility which is defined as,

$$\text{Utility}(D_{(\alpha,\beta)}) = -\sum_{a_1 \in A_1} \cdots \sum_{a_n \in A_n} P(a_1, \ldots, a_n) \log P(a_1, \ldots, a_n), \tag{10}$$

where $D_{(\alpha,\beta)}$ is the dataset based on the attributes in the sets Non-sensitive$_{(\alpha,\beta)}$ and Ambigious$_{(\alpha,\beta)}$, $A_1, A_2, \ldots, A_n$ represent the attributes of the dataset $D_{(\alpha,\beta)}$ and $a_1, a_2, \ldots, a_n$ are particular values of $A_1, A_2, \ldots, A_n$. We have different levels of information for different resultant datasets (which are created by considering various thresholds and the resulting three-way division of attribute).

4.1.4. Quantifying trade-off between stability and utility

The second quantitative aspect is the realization of a good balance between the number of attributes in the non-sensitive and ambiguous groups. For a certain three-way division of attributes, keeping majority of the attributes in the non-sensitive group puts the privacy of data at stake while considering more attributes in the ambiguous group will have a negative impact on the usefulness of the dataset. To incorporate this aspect into the selection of attribute division, we define the measure of stability which is defined as,

$$\text{Stability}(D_{(\alpha,\beta)}) = \frac{|\text{Non-Sensitive}_{(\alpha,\beta)}| \times |\text{Ambiguous}_{(\alpha,\beta)}|}{|At| \times (|\text{Ambiguous}_{(\alpha,\beta)}| + |\text{Non-Sensitive}_{(\alpha,\beta)}|)}. \tag{11}$$

Stability will have its minimum value when all the attributes (apart from the attributes of the sensitive group) are either in the non-sensitive or ambiguous groups. On the other hand, it will have its maximum value when the attributes are equally divided among the non-sensitive and ambiguous groups.

To incorporate both the measures of utility and stability into a single framework, we define another measure which we call suitability which is defined as,

$$\text{Suitability}(D_{(\alpha,\beta)}) = \frac{2}{\text{Utility}^{-1}(D_{(\alpha,\beta)}) + \text{Stability}^{-1}(D_{(\alpha,\beta)})}. \tag{12}$$

where $\text{Utility}^{-1}(D_{(\alpha,\beta)})$ and $\text{Stability}^{-1}(D_{(\alpha,\beta)})$ are the reciprocals of Utility and Stability respectively. The measure of suitability considers both utility and stability and we use it to select a suitable dataset as shown in Fig. 1.

The iterative change of thresholds for continuously improving the measure of suitability will provide useful hints towards optimal thresholds. In particular, different thresholds will lead to different datasets which are created by combining the resulting non-sensitive and ambiguous attributes (corresponding to the thresholds) and therefore will have different values for suitability. We proposed an algorithm in Section 4.3 for obtaining suitable thresholds defining the three-way attribute division based on the measure of suitability.

4.2. Demonstration of three-way division of attributes

In this section, we demonstrate with the help of an example the use of three-way division of attributes. We consider a sample dataset shown in Table 1 which is created based on the sample data taken from the Adult dataset. The sample dataset contains 12 attributes and 20 instances.

In order to apply the three-way attribute division, we first need to determine the evaluation function values for all the attributes. For this purpose, we compute entropy as in Eq. (6) for all the attributes. The entropy for a certain attribute for instance the attribute of Work can be computed as,

$$\begin{aligned}
\text{Entropy(Work)} &= -\sum_{a_i \in \text{Work}} P(a_i) \log P(a_i) \\
&= -\big(P(\text{Gov.}) \log P(\text{Gov.}) + P(\text{Self}) \log P(\text{Self}) + P(\text{Priv.}) \log P(\text{Priv.})\big) \\
&= -\left(\frac{2}{20} \times \log\left(\frac{2}{20}\right) + \frac{4}{20} \times \log\left(\frac{4}{20}\right) + \frac{14}{20} \times \log\left(\frac{14}{20}\right)\right) \\
&= 0.8
\end{aligned}$$

Entropy of other attributes can be computed in the same way. Table 2 lists all the values which are normalized in the range of $[0, 1]$ for the sake of ease in interpretation. We may note that the attribute Age has the highest entropy value in Table 2 because it has

Table 1
Sample data from the Adult dataset.

Age	Work	Edu	EduNo	Marital status	Occupation	Relationship	Race	Sex	Loss	Hpw	Country
39	Gov.	BS	13	Never	Clerk	Not-in-family	White	M	0	40	US
50	Self	BS	13	Civ-spouse	Manager	Husband	White	M	0	13	US
38	Priv.	HS	9	Divorced	Cleaner	Not-in-family	White	M	0	40	US
53	Priv.	11th	7	Civ-spouse	Cleaners	Husband	Black	M	0	40	US
28	Priv.	BS	13	Civ-spouse	Professor	Wife	Black	F	0	40	Cuba
37	Priv.	MS	14	Civ-spouse	Manager	Wife	White	F	0	40	US
49	Priv.	9th	5	Spouse-absent	Other	Not-in-family	Black	F	0	16	Jamaica
52	Self	HS	9	Civ-spouse	Manager	Husband	White	M	0	45	US
31	Priv.	MS	14	Never	Professor	Not-in-family	White	F	0	50	US
42	Priv.	BS	13	Civ-spouse	Manager	Husband	White	M	0	40	US
37	Priv.	College	10	Civ-spouse	Manager	Husband	Black	M	0	80	US
30	Gov.	BS	13	Civ-spouse	Professor	Husband	Asian	M	0	40	India
23	Priv.	BS	13	Never	Clerk	Own-child	White	F	0	30	US
32	Priv.	Acdm	12	Never	Sales	Not-in-family	Black	M	0	50	US
40	Priv.	Voc	11	Civ-spouse	Craft	Husband	Asian	M	0	40	China
34	Priv.	7th-8th	4	Civ-spouse	Transport	Husband	Asian	M	0	45	Mexico
25	Self	HS	9	Never	Farming	Own-child	White	M	0	35	US
32	Priv.	HS	9	Never	Inspector	Unmarried	White	M	0	40	US
38	Priv.	11th	7	Civ-spouse	Sales	Husband	White	M	0	50	US
43	Self	MS	14	Divorced	Manager	Unmarried	White	F	0	45	US

Table 2
Entropy of attributes for sample data.

Attributes	Entropy	Attributes	Entropy
Age	1.0	Relationship	0.50
Work	0.29	Race	0.34
Edu	0.70	Sex	0.22
EduNo	0.70	Loss	0.00
Marital status	0.38	Hpw	0.60
Occupation	0.75	Country	0.35

the maximum number of distinct values and therefore has the highest entropy. This attribute conveys the maximum information and needs to be placed in the sensitive group because one can easily infer a person's age using this attribute.

On the other hand, the attribute Loss has only a single value and therefore has a minimum entropy. This attribute may be placed in the non-sensitive group because little or no information about an individual may be inferred based on this attribute. Once the evaluation function values are computed, the three-way division of attributes is carried out using Eqs. (7)–(9). For a certain threshold pair, say $(\alpha, \beta) = (1,0)$, the division of attributes is given by,

$$\begin{aligned}
\text{Sensitive}_{(1,0)} &= \{\text{Age}\} \\
\text{Non-Sensitive}_{(1,0)} &= \{\text{Loss}\} \\
\text{Ambiguous}_{(1,0)} &= \{\text{Work, Edu, EduNo, Marital Status,} \\
&\quad \text{Occupation, Relationship, Race, Sex, Hpw, Country}\}
\end{aligned}$$

The resultant dataset given by $D_{(\alpha,\beta)}$ in this case will be created based on the attributes in the sets $\text{Non-Sensitive}_{(\alpha,\beta)}$ and $\text{Ambigous}_{(\alpha,\beta)}$. Since different thresholds will lead to different division of attributes, we need to compute thresholds based on qualitative aspects of the resultant dataset. The measures of utility, stability and suitability will be computed for this purpose which will reflect the effectiveness of the computed thresholds. The measure of utility for the thresholds of $(\alpha, \beta) = (1,0)$ is given by,

$$\text{Utility}(D_{(1,0)}) = -\sum_{a_1 \in \text{Loss}} \sum_{a_2 \in \text{Work}} \cdots \sum_{a_{11} \in \text{Country}} P(a_1, a_2, \ldots, a_{11}) \log P(a_1, a_2, \ldots, a_{11})$$

In the same way, the measure of stability and suitability for the same thresholds of $(\alpha, \beta) = (1,0)$ are given by,

$$\begin{aligned}
\text{Stability}(D_{(1,0)}) &= \frac{|\text{Non-Sensitive}_{(1,0)}| \times |\text{Ambiguous}_{(1,0)}|}{|At| \times (|\text{Ambiguous}_{(1,0)}| + |\text{Non-Sensitive}_{(1,0)}|)} \\
&= \frac{|\{\text{Loss}\}| \times |\{\text{Work, Edu, EduNo, } \ldots\}|}{|At| \times (|\{\text{Work, Edu, EduNo, } \ldots\}| + |\{\text{Loss}\}|)} \\
&= \frac{1 \times 10}{12 \times 10 \times 1} = 0.08 \\
\text{Suitability}(D_{(1,0)}) &= \frac{2}{\text{Utility}^{-1}(D_{(1,0)}) + \text{Stability}^{-1}(D_{(1,0)})} \\
&= \frac{2}{(0.9)^{-1} + (0.08)^{-1}} = 0.15
\end{aligned}$$

Table 3
Utility, Stability and Suitability of the dataset resulting from different thresholds.

(α, β)	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.5, 0.5)	0.20	0.17	0.18
(0.6, 0.4)	0.27	0.18	0.22
(0.7, 0.3)	**0.65**	**0.15**	**0.24**
(0.8, 0.2)	0.90	0.08	0.15
(0.9, 0.1)	0.90	0.08	0.15
(1.0, 0.0)	0.90	0.08	0.15

One can compute the respective values for all possible pairs of thresholds that may happen within the data. For the considered dataset, the values are given in Table 3. We can find a pair of thresholds with maximum value for the measure of suitability in the table which combines both the measures of utility and stability. For this example, in this case, the maximum value corresponds to $\alpha = 0.7$ and $\beta = 0.3$. This exhaustive search may not be possible for large datasets with many attributes and therefore in the next section, we present an algorithm for automatically determining the thresholds.

4.3. Three-way attribute division algorithm for differential privacy (3WADD)

In this section, we present a three-way decisions based algorithm for differential privacy called three-way attribute division for differential Privacy or 3WADD. Algorithm 1 presents the of 3WADD. The algorithm takes the original dataset D_o, thresholds (α, β) and step size λ as inputs and returns a publishable dataset D_p based on suitable three-way division of attributes.

Line 1 of the algorithm computes the utility of the original dataset D_o using Eq. (6). Line 2 makes a simple assignment to variables. From line 3 to 11, we repeatedly modify and refine the thresholds with the aim of improving the overall usefulness of the resultant dataset based on the measures discussed in Section 4.1. To do this, we first compute the three-way division of attributes in lines 5 to 7 which is followed by computing the resultant dataset given by $D_{\alpha,\beta}$ in line 8. Next, we compute the usefulness of the four neighboring thresholds using the Suitability measure. The threshold pair that yield the maximum suitability value is selected at each iteration. This helps in directing and guiding the search towards optimal thresholds.

Algorithm 1 Three-way attribute division for differential privacy

Input: Original Dataset D_o, thresholds (α, β), step size λ
Output: Publishable Dataset D_p
1: Compute Utility of D_o
2: $(\alpha', \beta') \leftarrow (\alpha, \beta)$
3: **do**
4: $(\alpha, \beta) \leftarrow (\alpha', \beta')$
5: $\text{Sensitive}_{(\alpha,\beta)} \leftarrow \{A_i \in At \mid e(A_i) \geq \alpha\}$
6: $\text{Non-Sensitive}_{(\alpha,\beta)} \leftarrow \{A_i \in At \mid e(A_i) \leq \beta\}$
7: $\text{Ambiguous}_{(\alpha,\beta)} \leftarrow \{A_i \in At \mid \beta < e(A_i) < \alpha\}$
8: $D_{(\alpha,\beta)} \leftarrow \text{Non-Sensitive}_{(\alpha,\beta)} \cup \text{Ambiguous}_{(\alpha,\beta)}$
9: $(\alpha', \beta') \leftarrow \max_{(\alpha,\beta)}(\text{Suitability}(D_{(\alpha-\lambda,\beta)}), \text{Suitability}(D_{(\alpha+\lambda,\beta)}),$
$\text{Suitability}(D_{(\alpha,\beta-\lambda)}), \text{Suitability}(D_{(\alpha,\beta+\lambda)}))$
10: **while** $(\text{Suitability}(D_{(\alpha',\beta')}) \geq \text{Suitability}(D_{(\alpha,\beta)})$
11: $D_{\text{Anonymized}_{(\alpha,\beta)}} \leftarrow$ Anonymize data corresponding to $\text{Ambiguous}_{(\alpha,\beta)}$ using differential privacy
12: $D_p \leftarrow D_{\text{Non-sensitive}_{(\alpha,\beta)}} \cup D_{\text{Anonymized}_{(\alpha,\beta)}}$
13: **return** D_p

Finally, in line 10, the algorithm checks if the suitability of the updated thresholds (α', β') is better than the suitability of the thresholds from the previous step. If they are better, the algorithm will continue and in any other case the algorithm will stop and the resultant thresholds will be the selected thresholds. In line 11, the dataset created with attributes in the set $\text{Ambigious}_{(\alpha,\beta)}$ is anonymized to create a dataset of $D_{Anonymized_{(\alpha,\beta)}}$ using the differential privacy mechanism explained in Section 2.1. Finally, the dataset corresponding to non-sensitive attributes, i.e., $D_{\text{Non-Sensitive}_{(\alpha,\beta)}}$ and the dataset corresponding to anonymized attributes are combined together to create a publishable dataset given by D_p.

5. Experiments and results

5.1. Experimental setup and datasets

The technique discussed in this paper is general and can even be applied to datasets gathered from sources other than IoT sensors. Therefore, we are using general as well as IoT sensor datasets to demonstrate our experiments. We used five datasets from the UCI machine learning repository and Kaggle repository in the experiments. These datasets include Titanic, Adult, Bank Marketing, Heart Disease and Student Performance. Some important information about these datasets is given in Table 4. It may be noted that different datasets have been used in the studies of differential privacy however there are no standard benchmarks. Generally speaking, the

Table 4
Datasets description.

Dataset	Attributes	Records
Titanic	12	1309
Adult	15	48,842
Bank Marketing	17	45,211
Heart Disease	14	720
Student Performance	30	1044

Table 5
Sample records for motion, light, pressure and contact sensors [25].

Sensor ID	Timestamp	Value	Name
5895	2020-05-04 12:55:45	0	Bathroom/ambience/motion
5887	2020-07-18 16:00:00	175	Kitchen/stove/light
5891	2020-07-28 16:00:00	0	Livingroom/ambience/motion
5892	2020-07-28 16:00:00	0	Bedroom/ambience/motion
6127	2020-07-28 16:00:00	1024	Livingroom/tv/light
5896	2020-07-28 16:00:00	555	Bedroom/bed/pressure
6687	2020-07-28 16:00:00	1	Bedroom/weightscale/pressure
5889	2020-07-28 16:00:00	6	Livingroom/couch/pressure
7125	2020-07-28 16:00:00	1024	Bathroom/ambience/light
5893	2020-07-28 16:00:00	0	Kitchen/ambience/motion
5888	2020-07-28 16:00:00	0	Entrance/door/contact
6686	2020-07-28 16:00:00	0	Bedroom/ambience_under_the_bed/motion
6220	2020-07-28 16:00:00	0	Balcon/door/contact
5894	2020-07-28 16:00:01	0	Corridor/ambience/motion
6253	2020-07-28 16:00:01	0	Kitchen/fridge/contact

Table 6
Summary of sensors, object monitored, and location. [25].

Sensor	Sensor type	Object monitored	Location
M06	Motion	Ambience	Bathroom
L01	Light	TV	Living room
L02	Light	Stove	Kitchen
L03	Light	Ambience	Bathroom
P01	Pressure	Couch	Living room
P02	Pressure	Bed	Bedroom
P03	Pressure	Weight scale	Bedroom
TH01	Temperature & Humidity	Ambience	Bathroom
D01	Reed switch	Door contact	Entrance
D02	Reed switch	Door contact	Balcon
D03	Reed switch	Fridge Door contact	Kitchen
SMP01	Smart plug	Coffee maker	Kitchen
SMP02	Smart plug	Dishwasher	Kitchen
SMP03	Smart plug	Sandwich maker	Kitchen
SMP04	Smart plug	Kettle	Kitchen
SMP05	Smart plug	Washing machine	Bathroom
SMP06	Smart plug	Microwave	Kitchen
SMP07	Smart plug	Vacuum cleaner	Corridor

datasets used in the previous studies are synthetic or artificially created for use in the specific studies and are not easily accessible. We selected publicly available datasets where the attributes can be meaningfully divided into three groups with clear semantic interpretation of the attributes belonging to the three attribute sets. These experiments can be performed on data from IoT sensors. One such dataset of human activities in a smart home environment is generated and discussed in [25]. Table 5 shows the data from light, motion, contact and pressure sensors. Table 6 shows the sensors, the object they are monitoring and their location in the house.

In all the experiments we use the starting thresholds of $(\alpha, \beta) = (0.5, 0.5)$. Different strategies may be employed with regards to the starting thresholds. We, however, used the initial setting of $(\alpha, \beta) = (0.5, 0.5)$ to examine the possible improvement in performance measures when there are no attributes in the ambiguous group. An important issue with regards to executing Algorithm 1 is the setting of suitable value for the step size λ. By having a higher values of λ, the Algorithm 1 may converge to the final result in lower number of iterations however the thresholds may not be very fine tuned. On the other hand, by having a lower value of λ, the Algorithm 1 may take more iterations to converge but it may allow to fine tune the thresholds. To use suitable and effective values of the thresholds, we tested different values of the λ on the considered datasets and noted the number of iterations the Algorithm 1 takes to converge to the final result. For each λ value, we noted the maximum and average number of iterations for the five datasets and report the results in Fig. 3. Note that we have a very higher number of iteration for lower values of λ but as

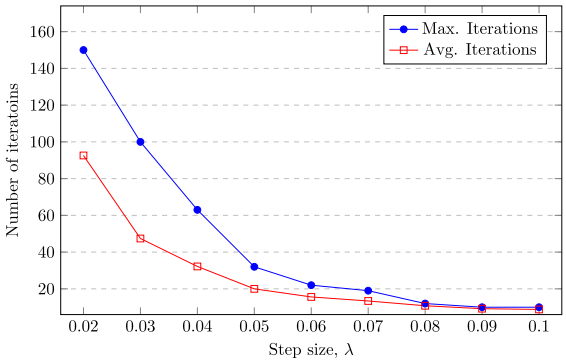

Fig. 3. Step size λ and number of iterations.

Table 7
Entropy of attributes of Titanic dataset.

Attributes	Entropy	Attributes	Entropy
Passengerid	1.0	Sibsp	0.039
Survived	0.0018	Parch	0.020
Pclass	0.054	Ticket	0.923
Name	1	Fare	0.658
Sex	0	Cabin	0.158
Age	0.477	Embarked	0.024

Table 8
Entropy of attributes of Adult dataset.

Attributes	Entropy	Attributes	Entropy
Age	0.529	Race	0.024
Workclass	0.116	Sex	0.038
Fnlwgt	1.0	Capital gain	0.024
Education	0.240	Capital loss	0
Education-num	0.240	Hours per week	0.297
Martial status	0.132	Country	0.035
Occupation	0.306	Target	0.027
Relationship	0.163		

Table 9
Distribution of attributes in three groups for the Titanic dataset.

(α, β)	Sen.$_{(\alpha,\beta)}$	Non-Sen.$_{(\alpha,\beta)}$	Amb.$_{(\alpha,\beta)}$	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.50, 0.50)	4	8	0	0.42	0.0	0
(0.50, 0.45)	4	7	1	0.42	0.07	0.12
(0.55, 0.45)	4	7	1	0.42	0.07	0.12
...	...	...	...	...	...	...
...	...	...	...	...	...	...
(0.95, 0.10)	2	6	4	0.72	0.2	0.31
(0.95, 0.05)	2	5	5	0.72	0.21	0.33

the λ increases, the algorithm converges in fewer iterations. We may also note that after around $\lambda = 0.05$, increasing the λ further has little or no change on the number of iterations. We therefore choose to use $\lambda = 0.05$ in all of our experiments.

5.2. Three-way attribute division results

The experiments are performed with the evaluation function of entropy. Please note that we use normalized values for entropy for all the attributes. Entropy of individual attributes of the Titanic dataset are given in Table 7. The highest entropy value is of the attribute named PassengerId. This is because each passenger has a unique identifier and therefore this attribute has the maximum amount of information or equivalently maximum entropy. On the other hand, attributes such as Sex and Survived has low entropy because the attribute Sex and Survived both have only two values of $\{\text{Male}, \text{Female}\}$ and $\{0, 1\}$ respectively. Entropy of individual attributes of the Adult dataset is given in Table 8. Similar trends can be found in the Adult dataset where some attributes have a larger entropy value hence carrying more information while others have low entropy and therefore carry lesser information.

Table 10
Distribution of attributes in three groups for the Adult dataset.

(α, β)	Sen.$_{(\alpha,\beta)}$	Non-Sen.$_{(\alpha,\beta)}$	Amb.$_{(\alpha,\beta)}$	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.50, 0.50)	2	13	0	0.68	0.0	0
(0.50, 0.45)	2	13	0	0.68	0.0	0
(0.55, 0.45)	1	13	1	0.79	0.06	0.11
...	...	...	...	...	...	...
...	...	...	...	...	...	...
(0.9, 0.05)	1	6	8	0.79	0.23	0.36
(0.95, 0.05)	1	6	8	0.79	0.23	0.36

Table 11
Distribution of attributes in three groups for the Bank Marketing dataset.

(α, β)	Sen.$_{(\alpha,\beta)}$	Non-Sen.$_{(\alpha,\beta)}$	Amb.$_{(\alpha,\beta)}$	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.50, 0.50)	3	14	0	0.59	0.0	0
(0.50, 0.45)	3	13	1	0.59	0.05	0.09
(0.55, 0.45)	2	13	2	0.68	0.1	0.17
...	...	...	...	...	...	...
...	...	...	...	...	...	...
(0.9, 0.15)	1	9	7	0.84	0.23	0.36
(0.95, 0.15)	1	9	7	0.84	0.23	0.36

Table 12
Distribution of attributes in three groups for the Heart Disease dataset.

(α, β)	Sen.$_{(\alpha,\beta)}$	Non-Sen.$_{(\alpha,\beta)}$	Amb.$_{(\alpha,\beta)}$	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.50, 0.50)	5	9	0	0.56	0.0	0
(0.50, 0.45)	5	9	0	0.56	0.0	0
(0.55, 0.45)	4	9	1	0.64	0.06	0.11
...	...	...	...	...	...	...
...	...	...	...	...	...	...
(0.9, 0.20)	2	7	5	0.8	0.21	0.33
(0.95, 0.20)	2	7	5	0.8	0.21	0.33

Table 13
Distribution of attributes in three groups for the Student Performance dataset.

(α, β)	Sen.$_{(\alpha,\beta)}$	Non-Sen.$_{(\alpha,\beta)}$	Amb.$_{(\alpha,\beta)}$	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
(0.50, 0.50)	10	20	0	0.71	0.0	0
(0.50, 0.45)	10	18	2	0.71	0.06	0.11
(0.55, 0.45)	9	18	3	0.74	0.09	0.16
...	...	...	...	...	...	...
...	...	...	...	...	...	...
(0.70, 0.3)	1	15	14	0.96	0.24	0.38
(0.70, 0.25)	1	14	15	0.96	0.24	0.38

Algorithm 1 is executed for all the datasets to compute effective thresholds and the respective three-way division of attributes. Table 9 shows the results corresponding to different iterations of the Algorithm 1 for the Titanic dataset. Each row of the table corresponds to a certain iteration of the algorithm. The last row of the table corresponds to the determined thresholds using Algorithm 1. When the algorithm starts all the attributes are crisply divided into sensitive or non-sensitive groups. As the algorithm iterates, the attributes from the sensitive and non-sensitive groups are moved to the ambiguous group. In particular, when the algorithm stops, the sensitive and non-sensitive groups are reduced by two and three attributes, respectively while the ambiguous attribute group increases by five attributes. The change of attributes among the different groups improves the measures of utility, stability and suitability. From the starting configuration of thresholds at the beginning of the algorithm that is $(\alpha, \beta) = (0.5, 0.5)$, the measure of utility improves by 30% with the determine thresholds of $(\alpha, \beta) = (0.95, 0.05)$. Moreover, the improvement in the measures of stability and suitably improve by 21% and 33% respectively.

Table 10 shows the results corresponding to the Adult dataset. The results are similar to those obtained for the Titanic dataset. Again we may note that as the algorithm iterates, the attributes are moved from the sensitive and non-sensitive groups to the ambiguous groups thereby reducing the size of sensitive and non-sensitive groups. In particular, the number of attributes in the sensitive group and non-sensitive groups are reduced by one and seven attributes respectively. The ambiguous group increases by eight attributes in this case. Change in number of attributes in the three groups may effect the measures of utility, stability and suitability. Therefore, the utility computed with starting thresholds improves from 0.68 to 0.79 with the computed thresholds $(\alpha, \beta) = (0.95, 0.05)$. On the other hand, both the stability and suitability are improved from 0 to 0.23 and 0.36, respectively. Similar results corresponding to the datasets of Bank Marketing, Heart Disease and Student Performance are reported in Tables 11–13.

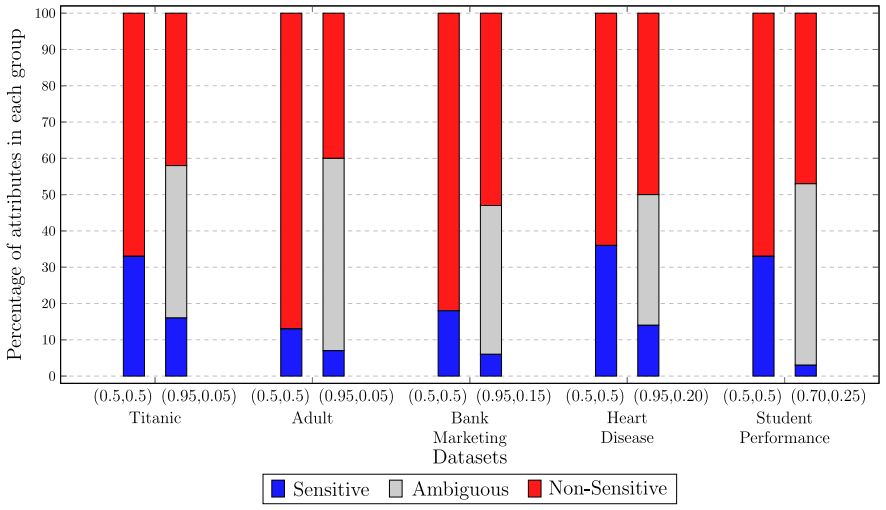

Fig. 4. Percentage of attributes in each group for (0.5, 0.5) and determined thresholds.

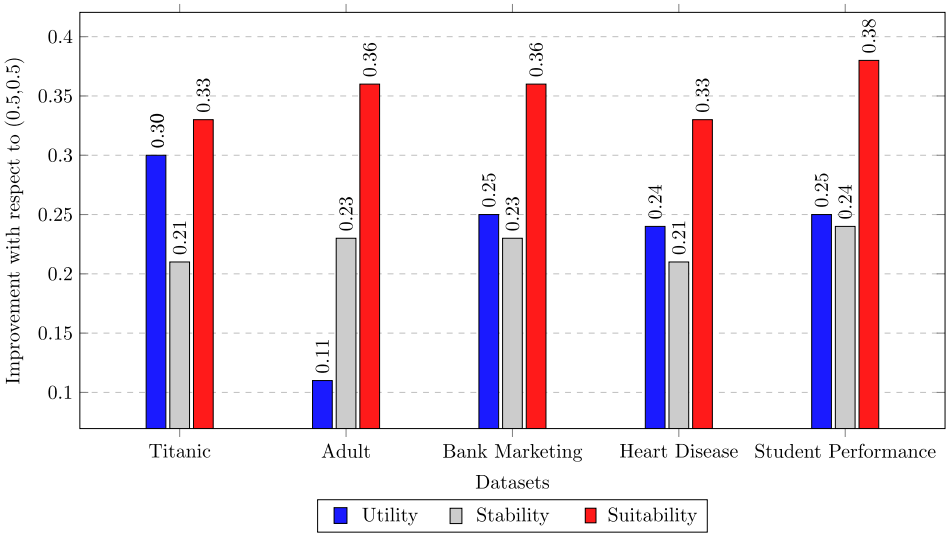

Fig. 5. Improvements in Utility, Stability and Suitability with respect to starting thresholds.

Figs. 4 and 5 are constructed to summarize the results in visual form. Fig. 4 shows the attributes group sizes for the initial and final computed thresholds. For all the datasets, the attribute division is refined based on three-way attribute division. Fig. 5 shows the percentage improvements in three measures with the determined thresholds from the starting or initial configuration of the thresholds. We may note that all three measures improve significantly with the determined thresholds. The measure of utility improves in the range of 0.11 to 0.3 for the considered datasets. There are also significant improvements in the measures of stability and suitability. In particular, the measure of stability shows an improvement in the range of 0.21 to 0.24 while the measure of suitability shows an improvement in the range of 0.33 to 0.38.

Table 14 shows the divisions selected by Algorithm 1 for each dataset. For the Titanic dataset, the suitable division is achieved by thresholds $(\alpha, \beta) = (0.95, 0.05)$. In this case, PassengerId and Name and are placed in the sensitive group. These attributes are perfect candidates for the sensitive group because publishing any of these attributes will cause sensitive information of an individual to be leaked. On the other hand, the attributes Survived, Sex, Sibsp (number of siblings/spouses aboard), Parch (number of parents/children abroad) and Embarked are placed in the non-sensitive group because none of these attribute may uniquely identify an individual in this case. For example, one cannot identify an individual's information based on the fact that he survived the crash or he was male or had certain number of children/parents aboard the ship.

Attributes like Age, Fare and Cabin are also sensitive but they also heavily contribute towards the utility of data and keeping them in the dataset is beneficial. These attributes may or may not determine an individual. For instance, there may be a single or multiple people with the same age. These attributes will be anonymized using differential privacy and then published. Similar

Table 14
Division of attributes with the determined thresholds.

Dataset	(α, β)	Groups	Entropy based division
Titanic	(0.95, 0.05)	$\text{Sensitive}_{(\alpha,\beta)}$	{Passengerid, Name}
		$\text{Non-Sensitive}_{(\alpha,\beta)}$	{Survived, Sex, Sibsp, Parch, Embarked}
		$\text{Ambiguous}_{(\alpha,\beta)}$	{Pclass, Age, Ticket, Fare, Cabin}
Adult	(0.95, 0.05)	$\text{Sensitive}_{(\alpha,\beta)}$	{fnlwgt}
		$\text{Non-Sensitive}_{(\alpha,\beta)}$	{Race, Sex, Capital gain, Capital loss, Country, Target}
		$\text{Ambiguous}_{(\alpha,\beta)}$	{Age, Workclass, Education, Education-num, Martial status, Occupation, Relationship, Hours per week}
Bank Marketing	(0.95, 0.15)	$\text{Sensitive}_{(\alpha,\beta)}$	{Balance}
		$\text{Non-Sensitive}_{(\alpha,\beta)}$	{Marital, Education, Default, Housing, Loan, Contact, Previous, Poutcome, Y}
		$\text{Ambiguous}_{(\alpha,\beta)}$	{Age, Job, Day, Month, Duration, Campaign, Pdays}
Heart Disease	(0.95, 0.20)	$\text{Sensitive}_{(\alpha,\beta)}$	{Chol, Thalach}
		$\text{Non-Sensitive}_{(\alpha,\beta)}$	{Sex, Cp, Fbs, Restecg, Exang, Ca, Num}
		$\text{Ambiguous}_{(\alpha,\beta)}$	{Age, Trestbps, Oldpeak, Slope, Thal}
Student Performance	(0.70, 0.25)	$\text{Sensitive}_{(\alpha,\beta)}$	{Absences}
		$\text{Non-Sensitive}_{(\alpha,\beta)}$	{School, Sex, Address, Famsize, Pstatus, Failures, Schoolsup, Famsup, Paid, Activities, Nursery, Higher, Internet, Romantic}
		$\text{Ambiguous}_{(\alpha,\beta)}$	{Age, Medu, Fedu, Mjob, Fjob, Reason, Guardian, Traveltime, Studytime, Famrel, Freetime, Goout', Dalc, Walc, Health }

Table 15
Comparison of the determined thresholds with extreme thresholds of (0.5,0.5) and (1,0).

Dataset	Thresholds	Utility($D_{(\alpha,\beta)}$)	Stability($D_{(\alpha,\beta)}$)	Suitability($D_{(\alpha,\beta)}$)
Titanic	(0.5, 0.5)	0.42	0.0	0.0
	(α, β)	0.72	**0.21**	**0.33**
	(1, 0)	**0.87**	0.08	0.15
Adult	(0.5, 0.5)	0.68	0.0	0.0
	(α, β)	**0.79**	**0.23**	**0.36**
	(1, 0)	**0.79**	0.06	0.11
Bank Marketing	(0.5, 0.5)	0.59	0.0	0
	(α, β)	**0.84**	**0.23**	**0.36**
	(1, 0)	**0.84**	0.06	0.11
Heart Disease	(0.5, 0.5)	0.56	0.0	0.0
	(α, β)	0.8	**0.21**	**0.33**
	(1, 0)	**0.91**	0.07	0.13
Student Performance	(0.5, 0.5)	0.71	0.0	0.0
	(α, β)	**0.96**	**0.24**	**0.38**
	(1, 0)	**0.96**	0.03	0.06

interpretation may be provided for the attributes in different groups corresponding to the other datasets shown in Table 14. These results show that our algorithm works effectively in identifying the attributes for the three groups.

5.3. Comparison with extreme thresholds

In this section, we provide comparative analysis of attribute division obtained with the determined threshold using Algorithm 1 and the extreme thresholds of $(\alpha, \beta) = (0.5, 0.5)$ and $(\alpha, \beta) = (1, 0)$. The casual reader may skip this section without loss of critical information.

The thresholds $(\alpha, \beta) = (0.5, 0.5)$ and $(\alpha, \beta) = (1, 0)$ are generally used as a starting point for learning effective thresholds of three-way decisions and comparisons with them provide useful hints for the performance gains that are achieved with the determined thresholds. It may be noted that with the thresholds setting of $(\alpha, \beta) = (0.5, 0.5)$, we have minimum possible size of the ambiguous attribute set while for the thresholds of $(\alpha, \beta) = (1, 0)$, we have maximum possible size of the ambiguous attribute set. Table 15 shows the evaluation measures for the extreme thresholds as well as the determined thresholds. We may note that with the determined thresholds, we always have better results compared to those of $(\alpha, \beta) = (0.5, 0.5)$. The configuration of $(\alpha, \beta) = (1, 0)$ has better utility especially for datasets of Titanic, Heart Disease and Student Performance, however, its stability and suitability is always inferior to those achieved with the determined thresholds.

The details results in this section advocate for the use of the proposed approach for obtaining automatic division of attributes for differential privacy.

6. Conclusion

The data collected and stored by sensors in Internet of things (IoT) needs to be protected against privacy breaches. Differential privacy is an approach for privacy preservation. Before applying differential privacy, it is necessary to divide the attribute set into three groups known as sensitive, non-sensitive and ambiguous. Existing practices rely on manual division of attributes by a domain expert and are therefore quite costly. We introduce a three-way approach for automatic attribute division for differential privacy. The approach divides the attribute set based on a pair of thresholds and an evaluation function. The configuration of thresholds controls the groupings or divisions of attributes and needs to be configured carefully. To achieve effective thresholds and the resulting grouping of attributes, we introduce an algorithm called 3WADD that automatically determines the thresholds for an effective division of attributes. An architecture that incorporated 3WADD using differential privacy is also presented. The proposed scheme improves the information content and stability of the dataset.

These results open up new research avenues for exploring more sophisticated methods of three-way decisions for obtaining effective and useful division of attributes for IoT. In particular, different kinds of evaluation functions may be explored depending on the underlying nature of the data and the specific needs of the application at hand. The automated nature of this approach can significantly reduce the cost of privacy preservation in an IoT dataset and thus motivate more organizations and individuals to use IoT to improve their processes.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was partially supported by faculty research support fund of NUCES, Pakistan.

References

[1] Martin KD, Kim JJ, Palmatier RW, Steinhoff L, Stewart DW, Walker BA, Wang Y, Weaven SK. Data privacy in retail. J Retail 2020;96(4):474–89.
[2] Alvim MS, Andrés ME, Chatzikokolakis K, Degano P, Palamidessi C. Differential privacy: on the trade-off between utility and information leakage. In: International workshop on formal aspects in security and trust. 2011, p. 39–54.
[3] Aravind K, Anand A, Sarath G. Inference detection in statistical database using frequent pattern. In: International conference on communication and signal processing. 2017, p. 1953–6.
[4] Hou J, Li XY, Jung T, Wang Y, Zheng D. Castle: Enhancing the utility of inequality query auditing without denial threats. IEEE Trans Inf Forensics Secur 2018;13(7):1656–69.
[5] Cormode G, Procopiuc CM, Shen E, Srivastava D, Yu T. Empirical privacy and empirical utility of anonymized data. In: International conference on data engineering workshops. 2013, p. 77–82.
[6] Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. L-diversity: Privacy beyond k-anonymity. ACM Trans Knowl Discov Data 2007;1(1):3–es.
[7] De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD. Unique in the crowd: The privacy bounds of human mobility. Sci Rep 2013;3(1):1–5.
[8] Tu Z, Zhao K, Xu F, Li Y, Su L, Jin D. Protecting trajectory from semantic attack considering k-anonymity, l-diversity, and t-closeness. IEEE Trans Netw Serv Manage 2018;16(1):264–78.
[9] Dwork C. Differential privacy: A survey of results. In: International conference on theory and applications of models of computation. 2008, p. 1–19.
[10] Lee J, Clifton C. How much is enough? choosing ϵ for differential privacy. In: International conference on information security. 2011, p. 325–40.
[11] Zhang S, Yang H, Singh L. Anonymizing query logs by differential privacy. In: International conference on research and development in information retrieval. 2016, p. 753–6.
[12] Wang T, Mei Y, Jia W, Zheng X, Wang G, Xie M. Edge-based differential privacy computing for sensor–cloud systems. J Parallel Distrib Comput 2020;136:75–85.
[13] Hassan MU, Rehmani MH, Chen J. Differential privacy in blockchain technology: A futuristic approach. J Parallel Distrib Comput 2020;145:50–74.
[14] Ren X, Yu C-M, Yu W, Yang S, Yang X, McCann JA, Philip SY. Lopub high-dimensional crowdsourced data publication with local differential privacy. IEEE Trans Inf Forensics Secur 2018;13(9):2151–66.
[15] Jung T, Jung K, Park S, Park S. A noise parameter configuration technique to mitigate detour inference attack on differential privacy. In: International conference on big data and smart computing. 2017, p. 186–92.
[16] Chen R, Fung BC, Yu PS, Desai BC. Correlated network data publication via differential privacy. Int J Very Large Data Bases 2014;23(4):653–76.
[17] Liu C, Chakraborty S, Mittal P. Dependence makes you vulnberable: Differential privacy under dependent tuples. In: Network and distributed system security symposium 16. 2016, p. 21–4.
[18] Bindschaedler V, Shokri R, Gunter CA. Plausible deniability for privacy-preserving data synthesis. Proc VLDB Endow 2017;10(5):481–92.
[19] Tamizhpoonguil B, Singh DAAG, Leavline EJ. Identifying sensitive attributes for preserving privacy. In: Artificial intelligence and evolutionary computations in engineering systems. Springer; 2017, p. 643–51.
[20] Ali B, Azam N, Shah A, Yao JT. A spatial filtering inspired three-way clustering approach with application to outlier detection. Internat J Approx Reason 2021;130:1–21.
[21] Xu J, Zhang Y, Miao D. Three-way confusion matrix for classification: A measure driven view. Inform Sci 2020;507:772–94.
[22] Fang Y, Min F. Cost-sensitive approximate attribute reduction with three-way decisions. Internat J Approx Reason 2019;104:148–65.
[23] Yao YY. Three-way granular computing, rough sets, and formal concept analysis. Internat J Approx Reason 2020;116:106–25.
[24] Smaldino PE. Measures of individual uncertainty for ecological models: Variance and entropy. Ecol Model 2013;254:50–3.
[25] Chimamiwa G, Alirezaie M, Pecora F, Loutfi A. Multi-sensor dataset of human activities in a smart home environment. Data Brief 2021;34:106632.

Waqas Ali is Lecturer with the Department of Computer Science, National University of Computer and Emerging Sciences, Pakistan. He received his master's degree in computer science from University of Peshawar in 2017. He currently is pursuing his Ph.D. in Computer Science from National University of Computer and Emerging Sciences, Pakistan. His research interest includes security and privacy.

Mohammad Nauman has a Ph.D. in security and privacy and a PostDoc in applications of machine learning to security and privacy. He has worked with many different languages, tools and platforms. His research has been published in journals and conferences of international repute. He has more than 1700 citations with an h-index of 17 and an i10 index of 25.

Nouman Azam is Associate Professor with the Department of Computer Science, National University of Computer and Emerging Sciences, Pakistan. He received a Ph.D. degree from the University of Regina in 2014. His research interests include rough sets, game theory, three-way decision making, decision support systems and multiple criteria decision analysis. He has over 30 scientific articles with over 900 citations.