A Differentially Private Index for Range Query Processing in Clouds
Cetin Sahin, Tristan Allard, Reza Akbarinia, Amr Abbadi, Esther Pacitti

To cite this version:

HAL Id: lirmm-01886725
https://hal-lirmm.ccsd.cnrs.fr/lirmm-01886725
Submitted on 3 Oct 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A Differentially Private Index for Range Query Processing in Clouds

Cetin Sahin, Tristan Allard, Reza Akbarinia, Amr El Abbadi, Esther Pacitti

Abstract—Performing non-aggregate range queries on cloud stored data, while achieving both privacy and efficiency is a challenging problem. This paper proposes constructing a differentially private index to an outsourced encrypted dataset. Efficiency is enabled by using a cleartext index structure to perform range queries. Security relies on both differential privacy (of the index) and semantic security (of the encrypted dataset). Our solution, PINED-RQ develops algorithms for building and updating the differentially private index. Compared to state-of-the-art secure index based range query processing approaches, PINED-RQ executes queries in the order of at least one magnitude faster. The security of PINED-RQ is proved and its efficiency is assessed by an extensive experimental validation.

I. INTRODUCTION

Substantial advances in cloud technologies have made outsourcing data to the cloud highly beneficial today. However, strong concerns from private companies and public institutions about the security of the outsourced data still hamper the adoption of cloud solutions. This reluctance is fed by frequent massive data breaches either caused by external attacks against cloud service providers or by negligent or opaque practices from the service provider.

During the last decade, a large body of academic work has tackled the problem of outsourcing databases to an untrusted cloud while maintaining both confidentiality and SQL-like querying functionality (at least partially). However, to the best of our knowledge, performing range queries efficiently in this context has not been addressed in a satisfactory manner. Range queries express a bounded restriction over the retrieved records. They are fundamental database operations. For example, assume that a university has outsourced its student database to the cloud. The following SQL query can retrieve the records of students with a grade between A and B: SELECT * FROM students WHERE grade ≥ 3.0 AND grade ≤ 4.0. Most related work has essentially focused on trading efficiency with security. In particular, they either allow unacceptable security leakage or employ costly cryptographic computations. For example, bucketization techniques [12] do not provide formal privacy guarantees and order preserving encryption based schemes (OPE) [2] are vulnerable to statistical attacks, while searchable symmetric encryption schemes [14], [5] suffer from execution times that are incompatible with real-world efficiency requirements.

In this paper, we advocate a novel efficient approach without sacrificing sound formal privacy guarantees. We build on the most recent advances in the field of privacy-preserving data publishing by using cryptography with differential privacy for performing selection range queries. Our solution proposes to send two complementary data structures to the cloud: an encrypted version of the database, e.g., AES encryption scheme, indexed by a hierarchy of histograms, such that both are perturbed to satisfy differential privacy. Efficiency comes from the disclosure of the index, in the clear, to the cloud, for guiding the query execution strategy. No computation is ever performed on encrypted data. Privacy comes from the differential privacy guarantees of the function that computes the encrypted database and the index. Indeed, the differential privacy model is today’s de facto standard for protecting personal information that needs to be partially disclosed. It applies to the functions computed on personal data, and defines privacy as a limit on the impact that any possible record may have on their outputs. This new efficiency/privacy trade-off, however, comes at a cost: the differentially private perturbation makes the index inaccurate. There may be some records that are relevant to the query that will not be retrieved (false negatives), and there may be some irrelevant records that will actually be returned (false positives). After receiving the result set, clients perform post-processing to filter out false positive records. This lower precision is the inevitable cost of increased privacy. A specific query processing strategy must be designed to cope with such inaccuracies, as well as an update management system to maintain the data structures when the original database is updated (inserts, deletes, or modifications of records) without jeopardizing the privacy guarantees.

We propose PINED-RQ (Privacy-preserving INdex for Encrypted Databases dedicated to Range Queries) which makes the following contributions:

1) A differentially private function computing the encrypted dataset and its hierarchical index.
2) An update strategy for managing the insertion, deletion, and modification of records on the cloud.
3) Formal proofs showing the security of PINED-RQ.
4) A thorough empirical evaluation demonstrating the efficiency and quality of the query processing strategy.

To the best of our knowledge, this is the first work that builds, uses, and maintains a differentially private index for performing selection range queries.
II. PROBLEM DEFINITION

A. Basic Components

Trusted Component. Raw data is produced by the data provider and queried by data consumers. The data provider encrypts the data and creates a differentially private index, which are sent to the cloud. Both the data provider and data consumers are trusted (see Figure 1), they are considered to be honest. For example, in a university setting, the data provider would be the university information system and the data consumers are the teachers and administrators.

Untrusted Component. The cloud is untrusted. It stores the data outsourced by the data provider and processes the queries posed by data consumers. We assume the cloud is honest-but-curious: it records all information resulting from its exchanges with the trusted components and may infer anything that can be inferred in a computationally-feasible way.

B. Basic Data Structures

The dataset stored by the data provider is a relation $\mathcal{D}(A_1, \ldots, A_d)$ where each $A_i$ is an attribute. Queries are non-aggregate single-dimensional range queries, over a single attribute $A_q$. A query $Q$ consists of a set of disjunctions of non-overlapping ranges over $A_q$: $Q \leftarrow \phi_1 \lor \ldots \lor \phi_l$ where each $\phi_i$ is a range defined by a minimum and a maximum value, such that $\cap_i \phi_i = \emptyset$. Without loss of generality, we assume a query $Q$ consists of a single range. Data Consumers submit queries in the clear to the cloud, without leading to any security breach. The attributes of $\mathcal{D}$ can be of any type, except $A_q$ which must be a totally ordered data type to allow range queries. The set of records in $\mathcal{D}$ that satisfy $Q$ exactly is called the set of relevant records and is denoted $\mathcal{R}$.

In order for the cloud to process queries, the data provider provides the following two data structures to the cloud:

- An encrypted version of the dataset denoted $\overline{\mathcal{D}}$. The encryption $\overline{r}$ of a record $r \in \mathcal{D}$ is performed by concatenating the attribute bit values of $r$ and encrypting the resulting bitstring by a semantically-secure encryption scheme [11], which means that no probabilistic polynomial-time algorithm is able to gain additional knowledge on a record given its encrypted version and (possibly) auxiliary information (e.g., AES in CBC mode). Loosely speaking, semantic security implies that no information leaks about a cleartext bitstring, given its encrypted value.
- An index, denoted $\mathcal{I}(A_q)$, over the queriable attribute of $\mathcal{D}$, $A_q$, computed from $\mathcal{D}$ but pointing to the encrypted records $\tau \in \overline{\mathcal{D}}$. The index is sent in the clear to the cloud.

The information in the nodes of the index is randomly perturbed so that differential privacy is satisfied.

The differentially private perturbation of the index results in an inherent approximation in the set of records that is returned: false positives may be returned while false negatives may be omitted. The recall and precision of an approximate set of records returned by the cloud are defined as follows.

Definition 1 (Recall and Precision): Given a query $Q$, with an exact set of relevant records $\mathcal{R}$ in $\mathcal{D}$, while the set of records returned by the cloud is $\mathcal{R}'$, then the recall $r$ and precision $p$ of $\mathcal{R}'$ are: $r = |\mathcal{R} \cap \mathcal{R}'|/|\mathcal{R}|$ and $p = |\mathcal{R} \cap \mathcal{R}'|/|\mathcal{R}'|$.

C. End-to-End Privacy Model

PINED-RQ combines a differentially-private perturbation scheme with a semantically-secure encryption scheme. Differential privacy and semantic security are two well-established models but each comes with its own formalism and assumptions. We first describe these two models in their usual settings, and then show how PINED-RQ integrates them consistently to come up with an overall unified end-to-end privacy model.

1) Traditional Differential Privacy: The $\epsilon$-differential privacy model [6] requires that whatever the output of an $\epsilon$-differentially private function, the probability that any given individual record $r \in \mathcal{D}(A_1, \ldots, A_n)$ is present in the dataset is close to the probability that $r$ is absent by an $e^\epsilon$ factor. This model considers a very strong adversary that is not computationally-bounded (information-theoretic guarantees). Definition 2 gives a formal definition.

Definition 2 ($\epsilon$-differential privacy [6], [8]): Randomized function $f$ satisfies $\epsilon$-differential privacy if:

$$\Pr[f(D_1) = O] \leq e^\epsilon \cdot \Pr[f(D_2) = O]$$

for any set $O \in \text{Range}(f)$ and any dataset $D_1$ and $D_2$ that differ in at most one record.

PINED-RQ perturbs the index $\mathcal{I}(A_q)$ based on the Laplace mechanism (Definition 3) and on the composability properties of the $\epsilon$-differential privacy model.

Definition 3 (Laplace mechanism [7]): Let $D_1$ and $D_2$ be two datasets such that $D_2$ is obtained from $D_1$ by changing the value of one record. Let $f$ be a real-valued function. Let $L(\lambda)$ denote a random variable which has a Laplace distribution with probability density function $p_{L}(x, \lambda) = \frac{1}{2\lambda} \cdot e^{-|x|/\lambda}$. The Laplace mechanism consists of adding $L(\max_n \Vert f(D_1) - f(D_2) \Vert_1/\epsilon)$ to the output of $f$, where $\epsilon > 0$.

Theorem 1 (Compositions [15]): Let $(f_1, \ldots, f_n)$ be a sequence of real-valued functions each satisfying $\epsilon_i$-differential privacy. This sequence of functions satisfies (1) $(\sum_i^{n} \epsilon_i)$-differential privacy when applied to the same dataset (sequential), and (2) $(\max(\epsilon_i))$-differential privacy when applied to disjoint datasets (parallel).

2) Traditional Semantic Security: Efficient private key encryption schemes today satisfy semantic security (e.g., AES in CBC mode). Loosely speaking, semantic security considers a computationally-bounded adversary, i.e., a probabilistic polynomial time algorithm, and requires that anything computable from the encrypted message and any auxiliary information,
e.g., obtained from another external data source, can also be computed efficiently from the auxiliary information only. Definition 4 is a simplification of Definition 5.2.1 in [10].

Definition 4 (Semantic security [10]): A private key encryption algorithm $E_\chi$, where $\chi$ is the secret key, is semantically secure if for every probabilistic polynomial time algorithm $A$ there exists a probabilistic polynomial time algorithm $A'$ such that for every input dataset $D$, every auxiliary background knowledge $\zeta \in \{0,1\}^*$, every polynomially bounded function $g : \{0,1\}^* \rightarrow \{0,1\}^*$, every polynomially bounded function $p(\cdot)$, and every sufficiently large $n \in N$, it holds that:

$$Pr[A_n(E_\chi(D), |D|, \zeta) = g(D)] < Pr[A'_n(|D|, \zeta) = g(D)] + \frac{1}{p(n)}$$

3) Unified Privacy Model for PINED-RQ: The unified privacy model of PINED-RQ is a probabilistic relaxation of a variant of differential privacy that considers computationally-bounded adversaries [16] and that consequently takes into account the cryptographically-negligible leaks due to the use of efficient real-world encryption schemes. Definition 5 is a simplification of $\epsilon_n$-SIM-CDP, the simulation-based computational differential privacy model proposed in [16].

Definition 5 ($\epsilon_n$-SIM-CDP privacy [16]): Randomized function $f_n$ provides $\epsilon_n$-SIM-CDP if there exists a function $F_n$ that satisfies $\epsilon_n$-differential-privacy and a polynomial $p(\cdot)$, such that for every input dataset $D$, every probabilistic polynomial time adversary $A$, every auxiliary background knowledge $\zeta \in \{0,1\}^*$, and every sufficiently large $n \in N$, it holds that:

$$Pr[A_n(f_n(D), |D|, \zeta) = 1] - Pr[A_n(F_n(D), |D|, \zeta) = 1] \leq \frac{1}{p(n)}$$

Finally, the overall end-to-end privacy model of PINED-RQ is stated in Definition 6.

Definition 6 ($(\epsilon, \delta)_n$-Probabilistic-SIM-CDP): A randomized function $f_n$ is said to provide $(\epsilon, \delta)_n$-Probabilistic-SIM-CDP if it provides $\epsilon_n$-SIM-CDP to each individual with probability greater than or equal to $\delta$, where $\delta \in [0, 1]$.

D. Problem in a Nutshell

We address the problem of designing the functions (1) CREATE, in charge of computing the two complementary data structures $I(A_q)$ and $D$, (2) INSERT and MOD/DEL, in charge of handling the updates over $D$, and (3) the query processing strategies of the cloud that answer cleartext range queries $Q$ while ensuring high recall and precision, (4) all that while satisfying $(\epsilon, \delta)_n$-Probabilistic-SIM-CDP.

III. STATIC CONTEXT: THE CREATE FUNCTION

In this section, we discuss the basic design of the PINED-RQ CREATE function and the corresponding query processing strategy in a read-only context. Throughout the section, we refer to the sample example depicted in Figure 2. The aim is to publish a student GPA dataset to a cloud server privately. The original dataset has 7 student records with GPAs from 0 to 4. Initially, a clear index is constructed for the dataset where leaf nodes point to the tuples with the corresponding GPA value. Then, the index entries are perturbed with differentially private noise which results in adding dummy records or deleting some records. In the example, 1 dummy record is inserted to the node with range [2, 3] and 1 dummy record is removed from the node with range [0, 1]. After the perturbation, the records are encrypted with a semantically secure encryption scheme. Finally, the cloud is provided the output of the CREATE function: namely, the encrypted dataset $D$ and the cleartext differentially private index $I(A_q)$ over $D$. In this section, we first describe the CREATE function, then prove that it satisfies the $(\epsilon, \delta)_n$-Probabilistic-SIM-CDP privacy model, and finally present a simple query execution strategy.

A. Data Structures Output by CREATE

We describe the two data structures provided to the cloud, and demonstrate the end-to-end security of the proposed system.

The first data structure computed by the data provider is the differentially private index. The design of this index must address the conflicting goals of allowing the retrieval of the records in a given range query while satisfying differential privacy. Both false negatives and positives are inherent, thus the challenge lies in reducing them to realistic numbers. To this end, we propose to benefit from two fruitful research tracks: on the one hand, from the B+Tree family of indices, widely used in traditional databases for supporting range queries, and on the other hand, from the more recent differentially private hierarchies of histograms, that have been shown to answer aggregate range queries accurately while satisfying differential privacy [18]. Index $I(A_q)$ is a balanced tree over the encrypted dataset $D$ in which each intermediate node contains a fixed-size set of pointers and each leaf node contains a set of pointers to the data records in $D$.

1) Basics: Nodes and Histograms: In a B+-Tree, a key is a single value, e.g., an integer, that indicates the range within which fall the records that can be accessed while following the associated pointers. In our context, rather than using single values as indications for ranges, we propose to use histograms. Indeed, histograms can be used as accurate estimators for ranges through the distributions they disclose. Histograms are defined in Definition 7. Histograms are also well known for integrating well with differential privacy [18]: the Laplace mechanism and the parallel composition theorem together allow adding a random variable sampled independently in $\mathcal{L}(1/\epsilon)$ to each bin in order to satisfy $\epsilon$-differential privacy.

Definition 7 (Histogram and Histogram Bins): Let $\Phi \leftarrow (\phi_1, \ldots, \phi_k)$ be a set of non-overlapping ranges that partition the domain of queriable attribute $A_q$. Each range $\phi_i \in \Phi$ is associated to its corresponding bin $b_i$ where $b_i$ stores the number of data records within the range of $\phi_i$. Each bin belongs to a unique node (as in Definition 8) in the index. A histogram $h$ is a complete set of bins over the entire domain.

Definition 8 (Node): A node is a histogram bin/pointer pair, where the pointer references either a child node or encrypted data records. Each node represents a bin of a histogram.
Considering the example from Figure 2, the index structure has 7 nodes where 4 of them are leaf nodes. The leaf nodes have histogram bins \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}. 4 leaf nodes together construct a complete histogram at the leaf level.

2) Building \(I(A_q)\): The hierarchy of nodes in the index structure is built following a three-step process. The first step computes the clear index, i.e., the nodes and the pointers. It does require a single pass over the clear dataset to associate each data record with the corresponding leaf node. Later, the hierarchy of the index is constructed considering the non-private branching factor, a system parameter of the structure. The second step perturbs the nodes of the index based on the Laplace mechanism to satisfy differential privacy and post-processes them in order to increase its utility. The third step encrypts the data records with a semantically secure encryption scheme after constructing the differentially private index. The dataset is scanned twice: 1) during the first step to construct the leaf nodes, a scan that is both necessary and sufficient for computing the histograms, and 2) during the encryption of data records. We explain now each step.

The first step computes each level of the hierarchy iteratively, starting from the leaf nodes at the bottom and ending with the single root node at the top. First, the leaf nodes (level 0) are instantiated. The number of leaf nodes is computed from the domain of the queriable attribute \(A_q\) and a unit-length interval that defines the length of each histogram bin. For example, if the attribute domain is from 0 to 100 and the unit-length interval is 1, then there are 100 leaf nodes with ranges \{\{0, 1\}, \{1, 2\}, \ldots, \{99, 100\}\}. Once the leaf nodes are created, then a scan of the cleartext dataset creates a pointer from the corresponding node to the data records and incrementing each bin’s counter by 1. When the scan is completed, the leaf nodes have the correct numbers with associated pointers to the actual data records. Considering the example in Figure 2, the leaf nodes of the clear index have counts \(3, 2, 1, 1\) for the corresponding ranges of \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}. This means there are 3 data records whose values are within the range of \{0, 1\} and the first leaf node has pointers to these records. All nodes together at the same level construct a complete histogram over the domain \([0, 4]\). The nodes of the upper levels are then computed such that each upper node points to a set of children nodes. The number of pointers that map to child nodes is set to the branching factor. The range of the bin of a node is a union of the children nodes’ ranges, i.e., given \(\Phi^0\) is the range partitioning of the leaf nodes \(\Phi^0 \leftarrow \{\phi_1^0, \ldots, \phi_m^0\}\), the upper level range partitioning of the domain is \(\Phi^1 \leftarrow \bigcup_{i=1}^m \left(\bigcup_{j=1}^b \phi_j^0\right)\). The count of the bin is computed by summing the counts of the child nodes. In our toy example, the upper node for the range \([0, 2]\) has a count of 5, which is the summation of two child nodes \([0, 1]\) and \([1, 2]\). As can be seen from the figure, the branching factor for the example is 2. This process goes on iteratively until a single node remains, which is the root node (highest level).

The second step perturbs the clear index to satisfy differential privacy. The differentially private computation of hierarchies of histograms has been extensively studied in the context of analytical queries. Although our context is different, PINED-RQ can benefit from the strategies proposed in [13], [4], [18] for distributing the privacy budget over the levels. Cormode et al. [4] compare a uniform budget allocation to a geometric budget allocation approach. The uniform budget allocation strategy allocates budgets to each level equally such that if the index has \(h\) levels, each level is allocated a budget of \(\epsilon/h\). In the geometric budget allocation, the allocated budget increases geometrically from the root to the leaves. The root receives the lowest budget, whereas the leaf nodes receive the highest budget. Cormode et al. demonstrate that geometric budgeting outperforms the uniform strategy as the height of an index increases. However, for shallower indexes \((h \leq 5)\), both strategies are competitive. Qardaji et al. [18] also explore the effect of privacy budget allocation and do not recommend optimizing the privacy budget allocation as long as the optimal branching factor is selected. Our approach also uses a uniform budget allocation strategy. The straightforward approach to apply differential privacy is to sample a random noise from the Laplace distribution for each node bin and add the sampled noise to the original count. The total privacy budget is denoted by \(\epsilon_{total}\). Consider the example discussed
before (Figure 2). The root node of the clear index has a count of 7 (range = [0, 4]). After the perturbation, the same node has a bin count of 8. This means the sampled noise for the bin is 1. Clearly, differential privacy causes a loss of utility in the index. Qardaji et al. [18] increase the utility of a histogram by generalizing the constrained inference approach proposed in [13]. The constrained inference provides consistency constraints between parent/children histograms, which has also been adopted by [4]. PINED-RQ also adopts the constrained inference approach to increase utility.

Unlike earlier approaches, we tackle a new problem while satisfying the differential privacy of the index. Earlier approaches target answering analytical range queries where the utility loss occurs due to the sampling of noises. However, the noise itself does not cause any problem since it only changes the count in the bins. This is also the case for the inner nodes in our index and our approach also updates the count of the node bins. However, in our context, the leaf nodes point to the data records which brings a novel challenge regarding noise sampling. We use the Laplace mechanism to sample noises and the sampled noises can be negative or positive as well. Therefore, our index construction handles two cases: 1) sampling of a positive noise, and 2) sampling of a negative noise, which are discussed next.

a) Positive noise sampling at leaf nodes: If the noise $v$ sampled from the Laplace mechanism is positive, $v$ dummy records are inserted at uniformly-random positions in the dataset and $v$ additional pointers from the leaf node to the dummy records are created. Assuming bin $b_i$ has a count of $c_i$, the updated count will be $c_i + v$. Note that each node in the index is perturbed separately and such a rule applies for each node that is perturbed with positive noise. Considering the example in Figure 2, the actual count of the node with bin range $[2, 3]$ is 1 in the clear index. This means there is only one real record in the real dataset that falls into this range. During perturbation, the sampled noise is $v = 1$ and the bin count of the same node in the differentially private index is 2. The differentially private index is outsourced to the cloud and the bin of the node is perturbed. Since the noise is sampled from the Laplace distribution, it can be selected based on the inverse of the cumulative distribution function (CDF) of the Laplace distribution. The size of the overflow array can be selected probabilistically large enough to store any removed records. Since the noise is sampled from the Laplace distribution, it can be selected based on the inverse of the cumulative distribution function (CDF) of the Laplace distribution with a very high probability. Note that it is possible for a sampled noise to be out of the selected bound. In this case, it is possible to append data records to their associated overflow arrays. This prevents PINED-RQ from missing the records. Later, we show that appending records to the associated overflow arrays does not violate PINED-RQ’s end-to-end privacy guarantee. Note that although overflow records from the overflow arrays are theoretically possible, it is very unlikely to happen if the size of the overflow array is selected large enough.

Setting the parameters. Our histogram-based index structure shares similarities with the hierarchy of histograms proposed in [18]. Two important parameters, branching factor and
number of bins, have a significant impact on the accuracy of the index. Qardaji et al. [18] discuss computing the branching factor and point out that when the number of bins is high, the optimal branching factor is around 16. The empirical analysis in [18] also highlights that the best performance is delivered when the branching factor is selected between 8 and 16. Therefore, we set the branching factor in PINED-RQ to 16.

B. Privacy Guarantees of the CREATE Function

We now show that the CREATE function of PINED-RQ satisfies $(\epsilon,\delta)$-Probabilistic-SIM-CDP as defined in Definition 6.

**Theorem 2:** Index $I(A_q)$ satisfies $\epsilon_{\text{total}}$-differential privacy (as defined in Definition 2) where $\epsilon_{\text{total}}$ is the budget dedicated to index perturbation, i.e., $\epsilon_{\text{total}} = \sum_{i=0}^{h} \epsilon_i$.

*Proof:* We consider neighboring datasets as two datasets, $D_1$ and $D_2$, differing in at most one record. Each node represents a bin of a histogram and a difference of a single record affects a maximum of one node: either increment or decrement count by 1. The maximum change 1 is used as a global sensitivity to sample noises from the Laplace distribution. Each bin is perturbed with a noise sampled from the Laplace mechanism, i.e., $\mathcal{L}(1/\epsilon_i)$. At each given level $l$, the set of bins (of histogram) satisfy $\epsilon_i$-differential privacy (parallel composition theorem). Second, any given root-to-leaf path satisfies $\sum_i \epsilon_i$-differential privacy. As a result, thanks to the distribution of the privacy budget, $\sum_i \epsilon_i = \epsilon_{\text{total}}$.

Moreover, since the composition of any function with a differentially-private function also satisfies differential privacy, the post-processing of the histograms in $I(A_q)$ also satisfies $\epsilon_{\text{total}}$-differential privacy. ■

Once PINED-RQ constructs the differentially private index, it encrypts each data record in $D$ and overflow arrays with a semantically secure symmetric encryption scheme parameterized with the secret key $\chi$ while preserving the pointer relation. The output of the encryption is the encrypted dataset $\mathcal{D}$ and encrypted overflow arrays. Note that semantic security guarantees that our computationally-bounded adversary has no way to distinguish encrypted dummy records from actual ones, neither in $\mathcal{D}$ nor in encrypted overflow arrays. We demonstrate in Theorem 3 the overall guarantees of the CREATE function.

**Theorem 3:** The CREATE function, in charge of computing $I(A_q)$, $\mathcal{D}$, and the overflow arrays satisfies $(\epsilon,\delta)_n$-Probabilistic-SIM-CDP as defined in Definition 6.

*Proof:* We have shown above (Theorem 2) that computing $I(A_q)$ satisfies $\epsilon_{\text{total}}$-differential privacy. We start with the computation of $\mathcal{D}$ and then consider the overflow arrays.

**Computation of $\mathcal{D}.$** First, the records in $\mathcal{D}$ are all encrypted with a semantically secure encryption scheme whether they are real records or dummy records. Loosely speaking, this means that a computationally-bounded adversary has negligible probability to distinguish encrypted real/dummy records from random bitstrings\(^2\). Due to this negligible leak, (information-theoretic) $\epsilon$-differential privacy is not satisfied anymore. We thus switch to the $\epsilon_n$-SIM-CDP computational analogue. Consider the pair made of the following two randomized functions: \(f^1\) that computes $I(A_q)$, and \(f^2\) that encrypts the real/dummy records and outputs $\mathcal{D}$. Consider the following equation: $\Pr[A_n(f^1_n(D,\zeta), f^2_n(D,\zeta)) = 1] - \Pr[A_n(F_n(D,\zeta)) = 1]$. First, it is easy to see that $\Pr[A_n(f^1_n(D,\zeta), f^2_n(D,\zeta)) = 1] = \Pr[A_n(f^1_n(D,\zeta)) = 1] + \Pr[A_n(f^2_n(D,\zeta)) = 1]$. Second, for $f^2_n$, the definition of semantic security (Definition 4) yields: $\Pr[A_n(f^2_n(D,\zeta)) = 1] < \Pr[A_n(\emptyset) = 1] + \frac{1}{\epsilon_{\text{total}}} = \frac{1}{\epsilon_{\text{total}}}$. Third, for $f^1_n$, we have $\Pr[A_n(f^1_n(D,\zeta)) = 1] - \Pr[A_n(F_n(D,\zeta)) = 1] = 0$ because both $F_n$ and $f^1_n$ are $\epsilon$-differentially private functions. As a result, $\Pr[A_n((f^1_n(D,\zeta), f^2_n(D,\zeta)) = 1] - \Pr[A_n(F_n(D,\zeta)) = 1] = \Pr[A_n(f^1_n(D,\zeta)) = 1] + \Pr[A_n(f^2_n(D,\zeta)) = 1] - \Pr[A_n(F_n(D,\zeta)) = 1] < \frac{1}{\epsilon_{\text{total}}}$. This is precisely the definition of $\epsilon_n$-SIM-CDP (Definition 5).

**Overflow arrays.** Finally, let introduce the overflow arrays. First, we consider the case where the number of removed records does not exceed the size of any overflow array. In that case, $\epsilon_n$-SIM-CDP is still satisfied because (1) there is exactly one overflow array per leaf, (2) each overflow array has the same size, and (3) all the records contained in an overflow array are encrypted by a semantically secure encryption scheme. Second, we consider the case where the number of removed records exceeds at least one overflow array. Note that this may happen only to the leaves that store a number of encrypted records higher than the capacity of an overflow array. Since the exceeding records are kept, appended to their corresponding overflow arrays, $\epsilon_n$-SIM-CDP is not satisfied anymore for the corresponding leaves. Fortunately, we are able to decide on the probability that this case occurs, say $\delta$, by computing from the Laplace cumulative distribution the minimum size that an overflow array should have to absorb negative noise. This results in satisfying $\epsilon_n$-SIM-CDP with a probability of $\delta$, which is precisely the definition of $(\epsilon,\delta)_n$-Probabilistic-SIM-CDP (Definition 6). ■

C. Query Processing Strategy

Static PINED-RQ deploys a simple query processing strategy to answer client requests. Given a range query, the query execution starts from the root of the index, and traverses the child of any node that has a non-negative intersection with the provided range. This is repeated recursively until the leaves of the index. In the leaf nodes, if a node has a positive count with the overlapping range query, then PINED-RQ returns the records pointed to by the corresponding node. If a leaf node is reached, independent of the node count, PINED-RQ returns the records in the overflow array for the corresponding node since PINED-RQ prioritizes high recall. Recall that PINED-RQ returns false positive and negative records in the result set. When data consumers receive the result set, they post-process to data to filter out the records that do not belong to the queried range. The remaining records are the set of correct results for the query.
A. General Approach

Assume a delete of record \( r_i \) is requested. PINED-RQ must handle this delete without compromising privacy. PINED-RQ does not remove the record from the published index and database - doing so would violate differential privacy (e.g., tagging or removing a record directly from the database would reveal that \( r_i \) is not a dummy record). Instead, the data provider maintains small databases, called \( \Delta DB \) and \( \Delta DB^j \) where \( i \) denotes the publication index and \( j \) denotes the \( j^{th} \) batch of modification/delete updates corresponding to the \( i^{th} \) publication (see Figure 3). PINED-RQ stores new insert operations in \( \Delta DB \). \( \Delta DB^j \) are used to store modifications and deletes corresponding to the \( i^{th} \) publication, i.e., \( \Delta DB^j \) and \( \Delta DB_{i+1} \) store updates related to the first publication. When the system is initialized and the initial dataset is published, the data provider stores modifications and deletes in \( \Delta DB_1 \). With incoming modifications and deletes, \( \Delta DB_1 \) grows and the data provider decides to publish \( \Delta DB_1 \) to the cloud at some point. After \( \Delta DB_1 \) is published to the cloud, the data provider stores modifications and deletes related to the first publication set in \( \Delta DB_2 \). Inserts, on the other hand, are batched in \( \Delta DB \), which also grows until the data provider decides to publish to the cloud as \( DB_2 \) with its associated index structure.

In PINED-RQ, each update operation is a new insert to either \( \Delta DB \) or one of the \( \Delta DB^j \) databases. When a new insert operation is requested, the data provider inserts it to \( \Delta DB \). Although such an action is obvious in the case of an insert operation, deletes and modifies result in inserting new records to the \( \Delta DB^j \) corresponding to the modified/deleted record. Each record has an additional attribute indicating the type of operation, i.e., insert, delete or modify. \( \Delta DB \) and \( \Delta DB_2 \) are initially empty and after some updates, differentially private indexes for them are created and then published to the server.

B. INSERT Function for handling inserts

An interesting feature of inserts that PINED-RQ exploits is that newly inserted records can be grouped together and each new group is associated with a new privacy budget. Considering the university example discussed before, each year new students register to the university without records in the published dataset. Instead of integrating new students to the previous publication, which would require using the partially consumed privacy budget, PINED-RQ associates these new students with a new publication and hence with a full new privacy budget.

1) Data Structures and Algorithms: Assume that the initially published dataset contains records with specific key values in attribute \( A_q \), denoted by \( \{ K_1, \ldots, K_m \} \). Note that a key might have multiple records in the database, e.g., records \( r_i \) and \( r_j \) might belong to \( K_1 \). Now consider an insert operation related to a new key \( K_{m+1} \). The data provider will note that there is no intersection with earlier publications regarding \( K_{m+1} \). Therefore, this new record can be associated with a new publication set. If there is an intersection with an earlier publication, the data provider would process \( K_{m+1} \) as a modify/delete. All keys \( K_{1..m} \) are related with the first publication; however, \( K_{m+1} \) is mapped to the second publication. The data provider stores new inserts in \( \Delta DB \) and, after processing some number of updates, it publishes \( \Delta DB \) to the cloud by constructing a secure index. Now, the cloud stores two encrypted databases, denoted by \( DB_1 \) and \( DB_2 \), and two differentially private indexes, \( DP-INDEX_1 \) and \( DP-INDEX_2 \), which point to \( DB_1 \) and \( DB_2 \), respectively. After this point, further insert operations will be associated with the
third publication. In this way, PINED-RQ can use separate privacy budgets \((\epsilon_{\text{total}}, \delta_{\text{total}})\) for each set of publications using parallel composition, which ensures differential privacy.

If the initial publication of a set of inserts consumes the full privacy budget \((\epsilon_{\text{total}}, \delta_{\text{total}})\), it is not possible to perform further publications associated with that publication set. To allow the system to continue publishing, the initial publication should use an initial \(\epsilon\) privacy budget denoted by \(\epsilon_{\text{init}}\) such that \(\epsilon_{\text{init}} < \epsilon_{\text{total}}\). The remaining budget is used to perform future publications.

2) Privacy Proof:

**Theorem 4:** The INSERT function satisfies \((\epsilon_{\text{total}}, \delta)\)-Probabilistic-SIM-CDP while processing inserts.

**Proof:** PINED-RQ stores new inserts in \(\Delta DB\). After some time, it creates a differentially private index DP-INDEX\(_i\) on \(\Delta DB\) by dedicating some privacy budget denoted by \(\epsilon_i\). The created index DP-INDEX\(_i\) is \(\epsilon_i\) differentially private. Given \(\epsilon_i \leq \epsilon_{\text{total}}\), DP-INDEX\(_i\) satisfies \(\epsilon_{\text{total}}\)-differential privacy. PINED-RQ creates each DP-INDEX\(_i\), on a disjoint dataset, hence from parallel composition (Theorem 1), PINED-RQ with the INSERT function is \((\max(\epsilon_i), \delta)\)-Probabilistic-SIM-CDP. Since \(\epsilon_i \leq \epsilon_{\text{total}}\), PINED-RQ with INSERT also satisfies \((\epsilon_{\text{total}}, \delta)\)-Probabilistic-SIM-CDP with new inserts.

C. MOD/DEL Function for Handling Modifies and Deletes

Assume a student objects to a grade after the grades have been submitted. As a consequence, this grade needs to be changed. As discussed earlier, a direct modification of a student’s grade in the published database violates privacy guarantees. Therefore, PINED-RQ stores updates related to previous publications in \(\Delta DB\), where \(i\) corresponds to the publication \(DB\), that contains the record corresponding to this student, and \(j\) refers to the \(j^{th}\) update batch of this publication.

Later, the data provider publishes these \(\Delta DB\) to the cloud. The main question is when to perform publications regarding modifications/deletes and how to allocate the privacy budget among multiple publications (publications to the same dataset need to share the same budget). Recall that the initial publication uses a privacy budget of \(\epsilon_{\text{init}}\). Hence, all future publications have to use the remaining privacy budget, denoted by \(\epsilon_{\text{rem}}\) where \(\epsilon_{\text{rem}} = \epsilon_{\text{total}} - \epsilon_{\text{init}}\), to create a differentially private index over \(\Delta DB\) and publish to the cloud. As stated earlier, it is possible to perform multiple \(\Delta DB\) publications. If this is the case, the remaining budget should also be shared among multiple \(\Delta DB\) publications. But the question is how?

1) When to Publish: The straightforward solution would be to perform periodic publications, i.e., after some fixed time or some fixed number of updates. The challenge with this approach is deciding on the parameters. It is obvious there is a trade-off between executing queries through the data provider and the server. Therefore, we consider the cost in the decision process for performing publications. The cost might depend on many external factors, e.g., location of servers, bandwidth, etc., but specifying these factors is beyond the scope of this paper. We assume there is a constant cost ratio between storing data at the data provider compared to the server, denoted by \(\alpha\). The decision is based on the following heuristic approach:

\[
\alpha \times \text{Relative Size} \times \left(1 + \frac{\epsilon_{\text{rem}}}{\epsilon_{\text{total}}}\right) \geq 2\mu
\]

where \(\text{Relative Size}\) is the ratio of the perturbed data size stored in the data provider compared to the server and \(\mu\) is a constant threshold parameter. \(\epsilon_{\text{rem}}\) is always less than or equal to \(\epsilon_{\text{total}}\), i.e., \(\epsilon_{\text{rem}}/\epsilon_{\text{total}} \leq 1\). Thus, the ratio on the left hand side \((1 + \epsilon_{\text{rem}}/\epsilon_{\text{total}}) \leq 2\). In the best case, this ratio is 2, therefore, \(\mu\) is multiplied by a constant factor of 2 to match the ratio \((1 + \epsilon_{\text{rem}}/\epsilon_{\text{total}})\).

2) Allocating the Privacy Budget: PINED-RQ allocates a privacy budget for the publication in a novel way. Previous works on differentially private updates were in the context of data streams, which have different characteristics. A notable exception is [20], which requires a system administrator to decide on the total number of publications \(k\) upfront, where each publication consists of updates in batches. The budget is split equally among publications (i.e., each publication receives \(\epsilon/k\)). However, this deterministic approach does not consider any external factors like dataset sizes. Thus, PINED-RQ uses the perturbed database size as a basis for allocation which considers the relative data storage at the data provider and \(\epsilon_{\text{rem}}\). Equations 2 and 3 compute the allocated privacy budget for \(\Delta DB\) together.

\[
\epsilon_{\Delta DB} = \epsilon_{\text{rem}} \times \frac{\text{Size}(\Delta DB)}{\text{Size}(DB) + \sum_{j=1}^{l} \Delta DB_j}
\]

As \(\epsilon_{\text{rem}}\) decreases, the system requires a higher ratio between the size of the storage at the data provider versus that in the cloud to perform publication. However, increasing this ratio results in storing more data in the data provider. Note that it is possible for Equation 2 to allocate very small budgets. Therefore, PINED-RQ allows a system administrator to set a minimum budget threshold for the allocated privacy budget denoted by \(\epsilon_{\text{min}}\). If \(\epsilon_{\Delta DB} < \epsilon_{\text{min}}\), the budget for publication \(\epsilon_{\Delta DB}\) is set to \(\epsilon_{\text{min}}\). To achieve higher utility, PINED-RQ uses a simple motivation, namely, less budget for bigger datasets, and more budget for smaller datasets.

\[
\epsilon_{\Delta DB} = \max(\epsilon_{\Delta DB}, \epsilon_{\text{min}})
\]

As each publication has its own budget, the data provider performs computations for each publication independently to decide on the publication of \(\Delta DB\) and its budget \(\epsilon_{\Delta DB}\).

3) Privacy Proof:

**Theorem 5:** PINED-RQ with the MOD/DEL function satisfies \((\epsilon_{\text{total}}, \delta^k)\)-Probabilistic-SIM-CDP with modifications and deletes, where \(k\) is the number of non-disjoint publications.
Proof: The modifications and deletes on the published dataset are also new inserts into $\Delta DB_i$, which is initially stored at the data provider. PINED-RQ applies a heuristic budget allocation mechanism for each publication, i.e., $\epsilon_{\text{total}} \geq \sum_{i=1}^{k} \epsilon_{\Delta DB_i}$ for any $i$ where $k$ is the number of publications on the set $i$. Hence, from sequential composition (Theorem 1), PINED-RQ satisfies $(\epsilon_{\text{total}}, \delta^k)$-Probabilistic-SIM-CDP while processing modifications and deletes.

D. Executing Queries

In the steady state, the server might have multiple indexes, e.g., $\text{DP-INDEX}_i, \text{DP-INDEX}_{i+1}, \text{DP-INDEX}_{i+2}, \text{DP-INDEX}_{i+k}$. Clients send queries to the data provider and the data provider partially answers the query based on its local information stored in $\Delta DB$ and $\Delta DB_i$. In addition, the data provider redirects the query to the server. To retrieve the latest state, the server might need to process a query over all indexes as the data might be deleted or modified. Since each index is independent, parallel execution is possible and existing parallel query execution strategies can be directly applied.

V. PERFORMANCE EVALUATION

This section presents experimental results that demonstrate the efficiency and practicality of PINED-RQ by examining the effects of varying system configuration parameters. We implemented PINED-RQ in Java. All experiments are conducted on a machine running Windows 7 with i5-2320 3 GHz CPU and 8 GB memory. The branching factor ($bf$) is set to 16 and the total privacy budget $\epsilon_{\text{total}}$ to 1. The domain of $A_q$ is normalized to $[0, 100]$. The size of overflow arrays is selected using the inverse of the CDF of the Laplace distribution for a given $\epsilon$ with 99.99% confidence interval.

Datasets. The experiments were performed with both synthetic and real datasets. To emulate real-world scenarios, the synthetic datasets follow two distributions: uniform or Zipfian with a skewness of 1, and contain 0.5 million records. For real datasets, we chose Gowalla [3], a social networking website where users share their locations by checking-in, and the US Postal Employees [1], USPS, dataset. The Gowalla dataset consists of 6, 442, 890 check-in records. For query attribute, we use the 32-bit integer representation of check-in times. The real datasets do not provide a perfect distribution so some of the nodes might cover very few records. If such nodes are perturbed with relatively high positive or low negative noises, the returned results include a number of false positive records or miss actual records. Therefore, the leaf nodes are more error-prone due to the added differentially private noise if a covered bin has a very low count. This is observed in Gowalla and USPS datasets. Some ranges have low counts and data removal causes query execution to suffer from low recall (e.g., as low as 85% for 5% range queries on the USPS dataset). This affects the overall recall performance for the USPS and Gowalla datasets. The removal of data records decreases recall for every dataset but is less observable for the synthetic datasets. The reason is that they follow almost a perfect distribution and leaf node bins have high enough counts (even the skewed one) which make the impact of removed records negligible. Although one can argue that PINED-RQ delivers good performance for the synthetic datasets even with no overflow array, real-world application/datasets usually do not follow perfect data distribution.

With Overflow Arrays. When PINED-RQ deploys overflow arrays, it achieves almost 100% recall for all cases except small ranges executed over Gowalla (see Figure 5). Recalls for small ranges are relatively high (98.6 – 98.8%). PINED-RQ misses some records since query execution stops traversing


### B. Skewness & Workload

When the data distribution is skewed, the precision performance of PINED-RQ is affected by the workload type (e.g., uniform, skewed). If a query range covers the skewed area, PINED-RQ delivers high recall and precision. We analyzed this case in more detail and Figure 6 presents our findings. We use datasets *Gowalla* and *USPS*, and two different workloads: *uniform* or *own*. The workload tag “own” means the query set that is executed over the dataset follows the same distribution as the dataset, and hence is skewed too. This is realistic, as it would be expected that the more dense areas of the dataset will be more often queried. The first part of the tag in the legend describes the dataset itself and the second part describes the type of workload used in the experiments. The executions of uniform randomly selected queries on Gowalla and USPS were presented in Figure 5 and discussed in the previous subsection. When the workload follows a dataset's distribution, the queries are generated randomly following this distribution. Independent of the underlying dataset and range size, PINED-RQ delivers high recall and precision when the workload follows the dataset’s own distribution. In all cases, both recall and precision are very close to 100%. This is not the case with uniform-randomly generated workloads, where performance depends on the queries. From our observations, precision and recall are quite high when the query range covers the skewed area and most of the queries in the skewed workloads cover the skewed area.

### C. Scalability

We use variants of the Gowalla dataset with a scaling factor of 0.5 million to test scalability. Figure 7 shows the results with increasing size. Each curve in the graph represents a different query size. Although there are small fluctuations in terms of recall and precision from 0.5 million to 1.5 million records for small queries, 1% and 5%, after 1.5 million, the recall value does not fluctuate and achieves almost 100% for all cases, which is quite significant. Larger dataset size means higher counts in the nodes. The magnitude of noise sampled from the Laplace mechanism is independent of the dataset size. Therefore, as the dataset size increases, the impact of the perturbation noise becomes negligible. This is a significant design advantage of PINED-RQ. The precision results are also less sensitive to changes in dataset size. In all cases, PINED-RQ achieves 99 – 100% precision, which is quite good from a system performance point of view.

### D. Effect of Epsilon

The effect of a privacy budget in differentially private publications has been studied by many prior works and it is known that smaller privacy budgets provide less utility, since...
This section evaluates the performance of PINED-RQ’s update management system. To simulate updates, we use an update-only uniform workload generator where 80% of the updates are new inserts, whereas the remaining 20% are modifications to earlier records. Due to the lack of space, we do not discuss the behavior of PINED-RQ for different update parameters. Here, we consider a specific scenario which fits well with the targeted application and evaluate PINED-RQ in terms of precision and recall. The results are presented in Figure 10. In this setting, we set $\epsilon_{\text{total}}$ to 1, the initial publication privacy budget $\epsilon_{\text{init}}$ to 0.7, the minimum publication budget $\epsilon_{\text{min}}$ to 0.3, the cost for storing data at the data provider $\alpha$ to 5, and the update frequency parameter $\mu$ to 2. The initial publication uses a synthetic uniform dataset of size 500k records. The system is tested after each publication to the server. To focus on the performance of indexes, the reported recall and precision rates do not consider the answers returned from the data provider (the results returned from the data provider have 100% recall and precision, which will obviously increase the recall and precision of query answers). The x-axis of the graphs in Figure 10 represents the publication id, i.e., the initial publication is denoted by $P_0$ and the next publication is denoted by $P_1$. There are 10 publications where nine of them are publications of inserts while $P_7$ is a special publication consisting solely of modifications to $P_0$, with a size of 307,693 records, on the initially published dataset.

The initial publication uses a budget of 0.7. This is also true for other publications except for $P_7$, which uses a budget of 0.3. Thanks to the parallel composition of differential privacy, PINED-RQ maintains its privacy while publishing new datasets with similar accuracy. Therefore, there is no significant effect on the performance of PINED-RQ while new datasets are published. The later publications only have a positive outcome since recall for the smallest range 1% starts from 99% with the initial publication and slightly increases with further updates. On the other hand, the precision for the same range is constant over the publications and is not affected by further publications. For all other ranges, PINED-RQ delivers decent performance with almost 100% recall and precision. Note that for each query, PINED-RQ scans all indexes in parallel, therefore, there is very small overhead in the index scan time compared to a single index case.

To compare our heuristic budget allocation mechanism, we ran experiments using the equal budget allocation [20]. Since there is no specific publication triggering mechanism in [20], we use PINED-RQ’s publication triggering mechanism for both systems. Considering the initial publication, there are 7 publications where $\epsilon_{\text{total}}$ is distributed. This experimental setup only considers modifications/deletes which relies on sequential composition. $\epsilon_{\text{init}}$ is set to 0.1. In this setup, PINED-RQ’s heuristic approach and the equal budget allocation provide approximately similar recall around 99.99%. The precision results are also very close to each other although our heuristic approach provides 0.1% more precision. This is simply the result of negligible noise sampling compared to the number of records on the leaves. When we ran similar experiments with a smaller dataset, e.g., 10k records, the difference between the two approaches is more obvious. PINED-RQ’s budget allocation strategy provides 3−4% more recall and 1% more precision, since the heuristic budget allocation strategy favors allocating more budget to the smaller dataset while the uniform budget allocation does not consider dataset size.
There have been many research efforts to improve the quality of privacy preserving histograms for aggregate queries, e.g., [18]. In our work, we take advantage of these results to improve the quality of the histograms used in the nodes of PINED-RQ. Bucketization has been used for answering range queries over outsourced data [12]. These approaches are complementary to ours as they can be used for optimal distribution of the encrypted data in the outsourced database. Order preserving encryption (OPE) and its variations [2] have been also used for range query processing. Unlike PINED-RQ, they reveal the underlying data distribution and are vulnerable to statistical attacks. Eu-Jin Goh [9] proposed a secure index that allows a user with a trapdoor for a data x to test if the database contains x or not. The index reveals no information about the data for which the user does not have the trapdoor. The objective of PINED-RQ index is different from that of [9] as it targets range queries instead of exact match queries. The recent works by Li et al. [14] and Demertzis et al. [5] rely on Searchable Symmetric Encryption (SSE). To take advantage of SSE, Demertzis et al. propose three types of indexing approaches the most secure approach of which has high space requirements, i.e., $O(n^2)$ where n is the database size and m the domain size. Even if the space requirement is improved, the proposed index scheme suffers from a high number of false positives along with execution times in the hundreds of seconds, unlike PINED-RQ which has execution times in the hundreds of milliseconds. The objective in [14], [5] is to provide index indistinguishability for the structure and node values in the index. PINED-RQ differs from this work in its objectives, as we aim at providing index differential privacy.

VI. RELATED WORK

REFERENCES


ACKNOWLEDGMENT

This work is partly supported by NSF grants CNS-1528178, CNS-1649469, the Inria Bigdatanet project, and the European Union’s Horizon 2020 - The EU Framework Programme for Research and Innovation 2014–2020, under grant agreement No. 732051.