https://doi.org/10.46335/IJIES.2021.6.8.2 **e-ISSN: 2456-3463**
Vol. 6, No. 8, 2021, PP. 4 - 11

International Journal of Innovations in Engineering and Science, www.ijies.net

Review on a Privacy-Preserving and Efficient k-Nearest Neighbor Model Based on k- Dimension Tree for Outsource Data

Pratiksha Bhimte[1], Neha Mogre[2]

[1] *P.G. Student,* [2] *Asst. Professor,* Department of Computer Science & Engineering, RTMN University, Nagpur ,India

***Received on**: 31 May, 2021* ***Revised on**: 30 June, 2021* ***Published on**: 02 July, 2021*

***Abstract –** Cloud computing technology has attracted the attention of researchers and organizations because of its computing power, efficiency and durability. Cloud computing technology is used to analyze exported data into a new data usage model. However, because of the major security risks arising from computer computing, many organizations now encrypt data before extracting data. So, in recent years, many functions in the k-Nearest Neighbor (indicated by k-NN) encrypted data algorithm have emerged. However, two major problems in the current study may be that the system is not secure enough or is not working properly. In this paper, based on existing issues, we are developing a non-KNN privacy protection plan and an integration plan. Our proposed scheme uses two existing encryption schemes: Order Keep Encryption and Parlier cryptosystem, encryption of encrypted encrypted data, data access patterns, and query recording, and use dimensional tree encryption (defined by kd-tree enhancement). traditional KNN algorithm. Our proposed system aims to achieve the effectiveness of queries while ensuring data security. The comprehensive test results prove that the system is very close to the system using written data and the existing system of encrypted data queries inconsistent with classification accuracy. ours is higher than the k-NN query scheme already in effect.*

Keywords-- Privacy preserving, k- nearest neighbor, k- dimensional tree, outsourced data.

I- INTRODUCTION

Nowadays, machine learning and cloud computing are widely used. Machine learning can include hidden information or patterns from big data and is one of the most attractive technologies. The K-Nearest Neighbor (shown by K-NN) algorithm is one of the oldest machine learning algorithms, which can get points closer to k from a set of big data based on the test object. It has been used in many subjects, such as pattern recognition, Location Based Services, DNA sequencing, online recommendation programs, and data analysis, etc. KNN firstly computes similarities between input query and each data in dataset (Compute Similarity), converts the similarities in bitwise shared representation (Bit-Decomposition), and selects K data with the highest similarities (PE-FTK). Among the sub protocols takes up more storage than the original data itself Until now, few computationally feasible solutions have been proposed for this scenario.

Update the feature extractor of a KNN model. Train a student model in the public Domain.

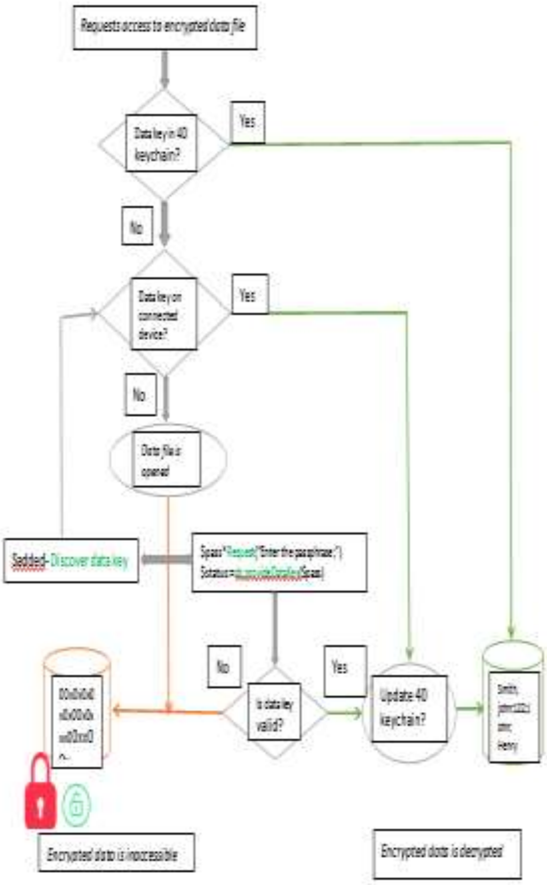
1. Update the feature extractor for private-KNN: We initialize the feature extractor with a public extractor --- Histogram of Oriented Gradient (HOG) features. We use the neural network of the last iteration student model (except for the last soft ax layer) to update the feature extractor, in the next iteration. Note that this interactive scheme will iteratively refine the feature embedding used by KNN without using any exclusive information.

2. Train a student model: When the feature extractor of Private-KNN is updated, we train a student model by labeling a limited number of student queries (the public data) with pseudo-labels. For each student query, we first generate a random subset from the entire private domain, and then pick the k nearest neighbors among the subset. The pseudo-label is generated with private voting of k neighbors, and the detailed aggregation process can be found in the main paper.

II- OBJECTIVES

The Private-KNN is the data-efficient algorithm for differentially private (DP) deep learning under the knowledge transfer framework. It represents the practical solution that addresses this important problem scales to larger models while preserving theoretically meaning full DP guarantee.

Fig 1: Architecture of NLP


Requests access to encrypted data file
Data key in 4D keychain?
Yes
No
Data key on connected device?
Yes
No
Data file is opened
$added- Discover data key
$pass="Request("Enter the passphrase:")
$status=
Is data key valid?
No
Yes
Update 4D keychain?
Smith, john123 ... Henry
Encrypted data is inaccessible
Encrypted data is decrypted

III -PROPOSED SYSTEM

The proposed system focus on solving the classification problem over encrypted data. In the proposed system, a new privacy preservation protocol based on KNN classification method is introduced to protect the confidentiality of data, privacy of user's input query and to hide the data access pattern. Figure 3.1 Architecture Using Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without the use of original data and provides data security in the cloud. The proposed algorithm for maintaining a close proximity neighbor and the partition process should not be displayed in the cloud server or other user. The proposed algorithm develops a privacy solution that keeps the k's privacy closer to encrypted data. In the access pattern. Figure 3.1 Creating confidential confidentiality is one of the most widely used data mining operations. Determines which results are closest indicating the low-grade category using neighbors closest to K. See Figure 3.1 for data privacy protection in the cloud. The new implementation of the privacy protection protocol for the recording of the encrypted query in the cloud encryption process is carried out in steps.

- Protected Data Security
- Question Processing
- Secure KNN query process

3.1 Protected Data Security The administrator is already required to register. Manager loads data in the cloud, before it has to be encrypted. Two types of data uploaded to the cloud. One is the standard query data (such as voter list data), and the second is the kNN query process (such as X and Y values). After that the user can be registered in the cloud. Registered users only have access to cloud data, so unauthorized access to secure data from cloud storage. Asymmetric-key algorithms require the use of asymmetric key pairs, consisting of a private key and corresponding public key. The key to be used for each operation depends on the cryptographic process being performed Each public / private key pair is associate with only one entity; this entity is known as the key-pair owner The public key may be known by anyone, whereas the private key must be known and used only by the key-pair owner. Key pairs are generated by the key-pair owner

3.2 Homomorphic Encryption The most common homomorphic encryption methods used for data encryption. in the cipher text and get the encrypted effect which when the encryption is removed is the same as the result of the sharp operation. Encryption Scheme has a four-step algorithm: Homomorphic Encryption = {key generation, encryption, encryption, keyword} Key Generation: KeyGen is an algorithm that generates pubic key, test key and secret key.

Encrypted data, Using the Homomorphic system, assigned two ciphertexts E (a) and E (b) of two meanings a and b respectively, encryption of their number E (a + b) can be calculated correctly by multiplying the key ciphertexts model key n2, i.e., E (a + b) = E (a) .E (b) mod n2.

Encryption - SK encryption is used for writing P text and then for Esk (pt) and the public key for writing this CT text will be sent to the server.

Decryption - removes the cipher C text with the secret key to retrieve P text.

Testing - removes cipher C of f (P) such as Decrypt (privk, P) = f (P). The scheme becomes Homomorphic if f can be any contradictory function, and the resulting text of the Test is cohesive.

That means it doesn't grow much without the difficulty of the job f. The test algorithm actually means that the scheme can test its pain algorithm. Homomorphic encryption has the best encryption method to ensure the security and privacy of shared information.

3.3 Question Processing After logging in user access to the standard query window. In the query process window, the user selects the data name, table name and access code of the data owner from the database. This process protects data privacy, user input question, and encryption the data access pattern. The user's input query will encrypted and pass to the cloud database. The cloud will classify label to corresponding query record. The query can retrieve the data from the cloud and show the encrypted and decrypted data in the output window.

3.4 Secure KNN query process An authorized user sends the encrypted query to cloud server. The proposed PPKNN protocol is to classify user's query record using encrypted database in a privacy preserving manner. The PPKNN protocol has: PPKNN(Encrypted Database(D1),Query(Q))->Class Label(Cq). Where Cq denotes the class label for Q after applying k-NN classification method on D1 and Q. The KNN classification algorithm is a machine learning algorithm. It is a method for classifying objects based on closest training samples in the feature space. KNN is a type of instance-based learning ; many test records will not be classified because they do not exactly the same as any other training record. The most sophisticated method, the closest segmentation of the nearest k (kNN), finds a group of objects in the training set closest to the test object, and supports the label allocation for a particular category in the area. There are three key elements of this method: a set of labeled items, e.g., a set of archived records, a distance or metric metric to calculate the distance between objects, and the value of k, the number of nearby neighbors. To distinguish an unlabeled item, the distance of this item from the labeled item is calculated, showing its closest neighbors, and then using the neighboring class labels to specify the category label of the item. The proposed PPKNN protocol mainly consists of two phases: Phase 1: Secure retrieval of neighbors close to K (SRKNN). At this stage, the authorized user submits a query (in encrypted form) to cover us. After this cloud is involved in a set of sub-protocols securely secured (encrypted) class labels that match the closest K-neighbors known only to cloud the server. Phase 2: Safe Mass Calculation (SCMCk). Following from Stage 1, the Cloud server will calculate the class label by voting more among the neighbors closest to the query.

IV- PROBLEM DEFINITION

Suppose that the owner of the data Alice is the owner of the data T for records, denoted by t1,. . . , tn, and signs m. Let ti, j show j the value of the recording. In our case, we assume that Alice initially secretly records her data quality, that is, she counts Epk (ti, j), $1 \le i \le n$ and $1\le j \le m$, where Epk means work public encryption key ecosystem secure. Allow encrypted database to be displayed by Epk (T). We think Alice is rolling out Epk (T) and future cloud processing services. Think of an authorized user Bob who wants to request the cloud of a neighbor's closest record in his input query Q = hq1 ,. . . , qmi based on Epk (T). During this process, Bob Q's query and database T content should not be disclosed in the cloud. In addition, data access patterns must be protected from the cloud. We refer to a process similar to the Secure kNN (SkNN) query for data encrypted to the cloud. Without a common loss, let ht 0 1,. . . , t0 k i means the nearest records k in Q. After that, we officially define the SkNN protocol as follows: SkNN (Epk (T), Q) → ht 0 1,. . . , t0 k i We emphasize that, at the end of the SkNN protocol, the result ht 0 1,. . . , t0 k i should only be displayed by Bob. We are now launching the actual SkNN protocol application. Example 1: Think of a doctor who wants to know the risk of heart disease in a particular patient. Allow T means heart rate sample with record-id symptoms, age, gender, cp, trestbps, chol, fbs, slope, th, and num as shown in Table I. Heart Database provided in Table I is available from the UCI machine learning library. Initially, the data owner (hospital) secretly writes that T claims to be smart, extracting encrypted Epk (T) data into the cloud for easy handling. In addition, the data owner sends future services for cloud query processing services. Now, we look at a doctor working in a hospital, says Bob, who would like to know the risk of heart disease in a particular T-based patient. Patient information details should be Q = h58, 1, 4, 133, 196, 1, 2, 1, 6i. In the SkNN protocol, Bob first needs to encrypt Q (to maintain the privacy of his query) and then send it to the cloud. Then the cloud searches the database encrypted with Epk (T) to find the neighbors closest to the user request. For simplicity, let us consider k = 2. Under this case, the 2 closest neighbors to Q are t4 and t5 (using the Euclidean range as a matrix for similarity). After this, the cloud sends t4 and t5 (encrypted) to Bob. Here, the cloud should point to the nearest neighbors of Q in an unobtrusive manner without knowing any sensitive information, that is, all statistics must be carried by encrypted records. Eventually, Bob gets t4 and t5 that will help him make treatment decisions.

V- OUR CONTRIBUTION

In this paper, we propose SkNN's novel process to simplify nearby neighborhood search for cloud-encrypted data that maintains data privacy and privacy query. In our protocol, when encrypted data is taken out of the cloud, Alice does not participate in any statistics. Therefore, no information was disclosed to Alice.

In particular, the law meets the following requirements:

- **Data confidentiality** - T content or other intermediate effects should not be disclosed in the cloud.
- **Question privacy** - Bob Q input question should not be disclosed in the cloud.
- **Accuracy** - Effect ht 0 1,. . . , t0 k i should only be displayed by Bob. In addition, no other information other than 0 0,. . . , T0 k should be revealed to Bob.
- **Low Computer Census for Bob** - After submitting his cloud-based question record, our agreements include a low accounting for Bob compared to existing jobs.
- **Hidden data access patterns** - Data access patterns, such as records that relate to their closest neighborsQ, should not be exposed to Alice and the cloud (to prevent any unnecessary attacks).

We emphasize that the intermediate effects seen by the cloud in our protocol may be random writing or random numbers. Therefore, which data records correspond to Q's closest neighbors known in the cloud. Also, after posting his secret question record in the cloud, Bob is not included in any of the statistics (low cost to Bob). Therefore, data access patterns are also secure to Bob. Some papers are arranged like this. We discuss the current work related to other background concepts in Section II. A set of security rights applied to the proposed protocols and their possible functionality are provided.

VI - RELATED WORK

Y. Du, "The effectiveness of a questionnaire that knows the privacy of location-based operations in Mobile Data Management, Reverse K adjacent to quiz processing questions: testing and analysis," VLDB Endowment developed a program for Wong et al. to provide confidential inquiries to NN. However, the data owner must participate in the query process, but the system does not have strong security evidence proposed by the k-NN query system based on the confidential homomorphism encryption system. In their scheme, the question of k-NN in encrypted data is found in homomorphic structures. How it is suggested how one can ensure personal privacy in relation to one's location and the proposed temporary conduct practices using a different privacy method that thinks the data path is secure and users can only ask for information based on it. The proposed plan outlines a way to maintain confidentiality in local archeology. However, he pointed out that both systems cannot withstand the selected attacks. Elmehdwi designed a homomorphic quiz based on NN with encrypted data. Although the data owner and client achieve privacy, computing and communication computers do not work well. A complex system of sublinear computation was recently proposed during the KN query process. The concept of Dp: A distinct diversity of independent human resources, ”in Processing of the 2015 ACM SIGSAC Conference on Computer and Communication Security. Private queries on location-based services: anonymizers are not required in Processing on ACM SIGMOD To check the nearest neighbor's question on road networks without leaking information on WISE2014.

VII - BACKGROUND

In this section, we introduce our two-dimensional cloud formation and define our enemy model and trust thinking. We also clarify the Secure k-NN problem in terms of which functions need to be encrypted in encrypted data, and we have briefly introduced the encryption of homomorphism, with the aim of making this paper self-contained.

7.1 Cloud Construction

The security effect of data extraction or computing on cloud servers requires careful study. There are many deployment options, including private cloud, public cloud and hybrid clouds. For businesses that place high value on data confidentiality and computer integrity, data extraction and computing may not be a legitimate risk. Independent cloud solutions address this need, with services available only within the enterprise intranet, with limited benefits of cloud computing such as required measurement and load balancing, as well as adding initial infrastructure and setup costs to new services. On the other side of the spectrum are public clouds, where large third-party farms are managed by servers and data centers that handle customer data and hiring accounting services. Two concerns are highlighted here: internal attacks, in which employees within a public enterprise can see and enter trade secrets, and side channels, e.g. Third-channel channels analysis is outside of this paper. The third model, the hybrid the cloud model uses the best of both worlds where depending on the sensitivity of the data and calculation, businesses can choose to launch only part of their services to the public cloud. Our Secure k-NN solution is targeted at public clouds. Basically, we are working on the so-called integrated cloud configuration, consisting of two unrelated public servers, introduced on the Twin Clouds and later implemented by the modern secure k-NN solution. Combined clouds are an example of the so-called middle clouds, a group of independent clouds in the world. Inter clouds allows for the best 1http: //archive.ics.uci.edu/ml/ to balance the load and allocation of resources to help and help deal with specific situations, e.g. Services that are specific to the region and require data to be stored in a specific geography. Integration of services across the central cloud can be localized, or seen as a peer as in the case of integrated clouds. A detailed study of cloud computing tax was introduced.

7.2 Guess of Trust

With integrated clouds, such as public clouds, the model of trust is that of a trustworthy person who is curious or a trustworthy enemy, who does not directly affect statistics or data. However, the enemy is free to view inputs and outputs, as well as negative effects of calculation and other behavioral features on cloud networks and servers. This type of enemy is different from the detective or malicious hateful model that was considered in the past, as the opponent is trusted to make an accurate calculation, but moreover is able to access the internal status of the service, which includes customer details. Such an enemy can view memory status, as well as network traffic, or learn the effectiveness of applications in answering customer queries. The choice of this particular type of enemy is justified, as data owners must relinquish this control to cloud service providers. Although this disclosure may be limited and governed by legal contracts and liabilities, the threat of curiosity cannot be denied. This is where using a computer directly over encrypted data fills a gap. The principle is that even though we are working on a model of loyal but ambitious enemies, a malicious intruder is unable to obtain plausible data from data or counting by sight. In addition, we want to prevent the enemy from reading database access patterns, such as a set of results (encrypted) returned answers related to a specific input query, and search query patterns, which may reveal details such as how often the same query was given. Given a trustworthy but curious enemy, the task of using the nearest k (NN) neighbors of a given query using a public cloud server, with the aim of achieving the above security objectives in the cloud space is difficult. One of the most attractive solutions is to use homomorphic encryption (HE). FHE (fully homomorphic encryption schemes allow conflicting activity counts on encrypted data. Using FHE, data owners can send their encrypted data to a public cloud, keeping all private or private key passwords. When a client submits a query, the query is encrypted using a secret key The same is then sent to the cloud server.All cloud servers are performed on encrypted data and the encrypted result is returned to customers, without compromising data confidentiality or accounting integrity, a reliable but curious enemy setting. Note that in this model, however, the actual algorithm, which is a computer sequence in data, is known internally, and is considered public. Care should be taken to design an algorithm to prevent leakage of search patterns and access patterns. Algorithm information should not reveal anything about the data, question or results. Such FHE schemes however come in importance operating costs and currently not working. For example, a state-of-the-art homomorphic sorting algorithm, it takes 2 minutes to process just 64 (32 bit) data objects, and as we show in our paper in section 5, we can safely calculate NN, with k = 2 of 30000 real data points (each point 23 sizes) simultaneously.

To address FHE performance issues, specific partia lHE ((S) HE and PHE) schemes have been proposed, which allow a set of tasks or sequences of encrypted data to work, so they work best. Examples include Paillier encryption (allowing encrypted encryption), LFHE, and BGN (which allows computer restriction restrictions on encrypted data). While using simple and efficient schemes with limited functionality, only a portion of the computer is made directly from encrypted data. Where more complex calculations are required, this should be done with precise values for intermediate outcomes. To do this, another cloud provider is installed on the protocol. This cloud service provider is also thought to be trustworthy - but curious - and has access to private keys that will allow you to define a partial accounting result. Using medium-sized transparency, complex operations are performed on these incomplete results, re-scanned and returned to the original cloud. The two clouds are not mutually exclusive, reasoning as these are public servers governed by legal contracts, and can be a business competitor. Working with each other will affect their reputation. This setting is called the integrated cloud model as described earlier. The challenge now is to show that knowledge of such intermediate results does not leak information about the actual details, question, results and access and search patterns. In this case, the status algorithm developed by Yourself teal., Shows that it is possible to design a secure k-NN system, where some secrets are assigned to one of the cloud servers, but both cloud servers learn nothing about real data. Our work also uses this model but examines the structure of the novel using the HE system (S), as well as an efficient protocol, which allows for unlimited implementation or real-world conditions.

7.3 Crucified Crucifixion

To find the nearest neighbors k, the distance between a given point and all other points in the database needs to be calculated (by the appropriate size and scale). For the Euclidean range say the spacing that means, between two points (x1, q y1) and (x2, y2) we need to calculate (x2 - x1) 2 + (y2 - y1) 2). For the purpose of computer efficiency, we can avoid the operation of square roots and operate with Euclidean squares. This calculation requires subtracting, making squares and adding that way. After calculating the Euclidean square distances in the cloud, we need to find the lowest values k. This requires that we order encrypted values. The Order Preservation Encryption (OPE), which was first proposed, also appears as an important area for new research. Using OPE, it is possible for the viewer to calculate the order between the two cipher texts without taking it out of the cave. Any OPE solution therefore automatically exceeds the original expulsion order between encrypted cipher scripts even if it does not specify the number of plaintexts themselves. OPE solutions themselves are not enough for our problem, because our definition of Secure k-NN does not allow the enemy to learn anything about the initial points or question, and the points should be at the level that the server orders after using computer ranges. In it it has been shown that a secure solution for kNN in a single cloud model clearly means that a secure OPE solution exists in this context, which does not disclose any information, including the order itself, expressed in the description, and this is not possible. (S) HE schemes on the other hand offer more functionality (rather than simple OPE) on encrypted data, and can be used cleverly to build a secure k-NN scheme.

VIII -TECHNIQUES

In the paper, use UDA to train the student model for SVHN and CIFAR-10 tasks, which allows us to save the privacy budget with a limited number of student queries. RKNN Query Answer Retrieval Algorithm used it.

Encryption method maintains privacy:

In this system, the cloud cannot detect the amount of any data (including question data records) because we use two encryption schemes, the encryption phase, or how many different classes in the scheme. And all results in the middle of the query result are encrypted data, and the cloud server can't read their bitter information. Therefore, the encryption process maintains privacy.

Privacy of Encrypted Data Comparison System

The data comparison protocol is an integral part of the k-NN query algorithm. As mentioned earlier, the comparative process state extensively using real datasets studying the effect of several parameters on computational cost and data overhead size. Our results show the efficiency and effectiveness of our solutions. Our future work includes extending our solutions for Dichromatic RKNN queries and moving object queries for spatial crowd sourcing applications while protecting the location privacy of the participants**.** OPE and Parlier cryptosystem, to encrypt the raw data and execute the k-NN algorithm. As mentioned earlier, a reliable cloud-but-curious cloud server cannot detect any information about its use in the kd tree process and distance comparisons. In our proposed program, we used the k-NN algorithm and the countless OPE system introduced in 2011. From this protocol, we can only compare the two details enclosed E (a) and E (b) without leaking any of the written values of a and b. Therefore, the cloud server cannot directly detect transparent data content. Similarly, with unauthorized users. Therefore, this comparison protocol maintains privacy.

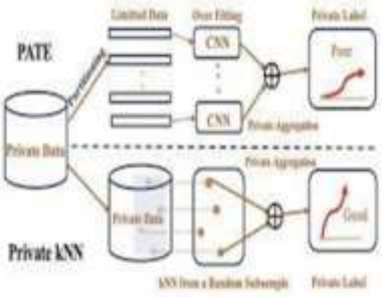


Fig 2- Proposed work model

IX- EFFECTS

The proposed plan has been tested with an attacker protection program. In a basic attack to protect players, there are two areas, the defender and the attacker. To make it easier to define, it has been tested on various networks. When an attacker tries to interfere with the network, then a protective action is taken. But the reward for the attackers is based solely on the expected outcome of the action. Based on these ideas, the probability of entry will vary from 0 to 1 and will be evaluated in a variety of contexts. Defender gain is based on the expected loss of the attack and restitution

X- CONCLUSION

In this paper, two novel solutions RKNN-HGnad RKNN-HRT have been suggested to answer RKNN's private questions without disclosing any information about the location of the question area. Our solutions use encrypted retrieval (PIR) to request data from an unreliable data server without the server learning about the retrieved data or query source. We tested our methods extensively using real data sets studying the effect of multiple parameters on computer costs and data size above. Our results demonstrate our effectiveness and our solutions. Our future work includes expanding our solutions for Bichromatic RKNN queries and submission inquiries for crowd access applications while protecting the privacy of participants' premises.

REFERENCES

[1] *Y. Du, "Privacy-aware run query processing location-based services," in Mobile Data Management. IEEE, 2016, pp253-257.*

[2] *B. Balle, G. Barthe, and M. Gaboardi. Privacy amplification by sub sampling: Tight analyses via couplings and divergences. In Preprint, 2018.*

[3] *R. Bassily, A. Smith, and A. Thakurta. Private empirical risk minimization: Efficient algorithms and tight error bounds. In Foundations of Computer Science (FOCS-14), pages 464–473. IEEE,2014.*

[4] *M. Bun and T. Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds.*

[5] *In Theory of Cryptography Conference, pages 635–658. Springer,2016.*

[6] *N. Carlini, C. Liu, U. Erlingsson, J. Kos, and D. Song. The ´ secret sharer: Evaluating and testing unintended memorization in neural networks. In 28th USENIX Security Symposium (USENIX Security 19), pages 267–284, Santa Clara, CA, Aug. 2019. USENIX Association.*

[7] *K. Chaudhuri, C. Monteleoni, and A. D. Sarwate. Differentially private empirical risk minimization. The Journal of Machine Learning Research, 12:1069–1109, 2011.*

[8] *T. Cover and P. Hart. Nearest neighbor pattern classification. IEEE transactions on information theory, 13(1):21–27,1967.*

[9] *N. Dalal and B. Triggs. Histograms of oriented gradients for human detection. 2005.*

[10] *C. Dimitrakakis, B. Nelson, A. Mitrokotsa, and B. I. Rubinstein. Robust and private bayesian inference. In Algorithmic Learning Theory, pages 291–305. Springer, 2014.1.*

[11] *C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In Theory of cryptography, pages 265–284. Springer,2006.*

[12] *C. Dwork, G. N. Rothblum, and S. Vadhan. Boosting and differential privacy. In Foundations of Computer Science (FOCS), 2010 51st Annual IEEE Symposium on, pages 51–60. IEEE,2010.*

[13] *S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith. What can we learn privately? SIAM Journal on Computing, 40(3):793–826, 2011.1.*

[14] *Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner. Gradientbased learning applied to document recognition. In Proceedings of the IEEE,1998.*

[15] *Z. Liu, P. Luo, X. Wang, and X. Tang. Deep learning face attributes in the wild. In ICCV,2015.*

[16] *Renyi differential privacy. In ´ 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pages 263–275. IEEE,2017.*

[17] *Mironov. Renyi differential privacy. In ´ Computer Security Foundations Symposium (CSF), 2017 IEEE 30th.*

[18] *https://web.mst.edu/~wjiang/SkNN-ICDE14.pdf*