Implementing Book Recommendation Using Machine Learning

Umarani C[1], Saranya S[2], Saranya N[3], Shobika[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] Kingston Engineering College , Vellore-59

Abstract- *In private publication agencies there are several dishonest publishers.To detect dishonest publishers there are several techniques were used.*

These techniques have less efficiency and low security.

Hence we propose a diffpart-differentially private scheme to check privately ,the correctness of the publishers. Our proposed machine learning based book recommendation system uses Tensorflow,k-means and linear regression method to detect dishonest publish

Keywords- Machine Learning, k-means clustering, Linear Regression, Tensor flow

I. INTRODUCTION

In this process, how to protect users' privacy is extremely critical. This is the so-called privacy preserving collaborative data publishing problem. A lot of privacy models and corresponding anonymization mechanisms have been proposed in the literature such as *k*-anonymity and differential privacy. *k*-anonymity and its variants (e.g. *l*-diversity and *t*-closeness protect)privacy by generalizing the records such that they can not be distinguished from some other records. Differential privacy is a much more rigorous privacy model. It requires that the released data is insensitive to the addition or removal of a single record. To implement this model, the corresponding anonymization mechanisms usually have to add noise to the published data, or probabilistically generalize the raw data. Obviously, all these data anonymization mechanisms have serious side effects on the data utility. As a result, the users of the published data usually have a strong demand to verify the real utility of the anonymized data

II. LITERATURE SURVEY

TITLE :Anonymous Credentials on a Standard Java Card
AUTHOR : Patrik Bichsel, Jan Camenisch, Thomas Groß, Victor Shoup
YEAR : 2009
DESCRIPTION:

Secure identity tokens such as Electronic Identity (eID)cards are emerging everywhere. At the same time user centric identity management gains acceptance. Anonymous credential schemes are the optimal realization of user centricity. However, on inexpensive hardware platforms, typically used for eID cards, these schemes could not be made to meet the necessary requirements such as future proof key lengths and transaction times on the order of 10 seconds. The reasons for this is the need for the hardware platform to be standardized and certified. Therefore an implementation is only possible as a Java Card applet. This results in severe restrictions: little memory (transient and persistent), an 8-bit CPU, and access to hardware acceleration for cryptographic operations only by defined interfaces such as RSA encryption operations.

TITLE : Cipher text policy Attribute based Encryption with anonymous access policy
AUTHOR :A.Balu1, K. Kuppusamy
YEAR : 2013
DESCRIPTION :

In Cipher text Policy Attribute based Encryption scheme, the encryptor can fix the policy, whocan decrypt the encrypted message. The policy can be formed with the help of attributes. In CP ABE, access policy is sent along with the cipher text. We propose a method in which the access policy need not be sent along with the cipher text, by which we are able to preserve the privacy of the encryptor. The proposed construction is provably secure under Decision Bilinear Diffe-Hellman assumption.

TITLE : Fine-Grained Access Control System based onOutsourced Attribute-based Encryption.
AUTHOR :Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, Wenjing Lou
YEAR :2010
DESCRIPTION :

As cloud computing becomes prevalent, more and more sen- sitive data is being centralized into the cloud for sharing, which brings forth new challenges for outsourced data security and privacy. Attribute- based encryption (ABE) is a

promising cryptographic primitive, which has been widely applied to design _ne-grained access control system re- cently. However, ABE is being criticized for its high scheme overhead as the computational cost grows with the complexity of the access formula. This disadvantage becomes more serious for mobile devices because they have constrained computing resources.

TITLE : Robust Threshold DSS Signatures
AUTHOR : Rosario Gennaro , Stanisław Jarecki, Hugo Krawczyk, Tal Rabin
YEAR : 2010
DESCRIPTION :

We present threshold DSS (Digital Signature Standard) signatures where the power to sign is shared by n players such that for a given parameter t<n=2 any subset of 2t+1signers can collaborate to produce a valid DSS signature on any given message, but no subset of t corrupted players can forge a signature (in particular, cannot learn the signature key). In addition, we present a robust threshold DSS scheme that can also tolerate n=3players who refuse to participate in the signature protocol. We can also endure =4maliciously faulty players that generate incorrect partial signatures at the time of signature computation. This results in a highly secure and resilient DSS signature system applicable to the protection of the secret signature key, the prevention of forgery, and increased system availability. Our results significantly improve over a recent result by Langford from CRYPTO'95 that presents threshold DSS signatures which can stand much smaller subsets of corrupted players, namely, t_pn, and do not enjoy the robustness property. As in the case of Langford's result, our schemes require no trusted party. Our techniques apply to other threshold ElGamal-like signatures as well. We prove the security of our schemes solely based on the hardness of forging a regular DSS signature.

TITLE : Distributed Pseudo-random Functions and KDCs
AUTHOR : Moni Naor, Benny Pinkas, and Omer Reingold
YEAR : 2009
DESCRIPTION :

This work describes schemes for distributing between n ser- vers the evaluation of a function which is an approximation to a random function, such that only authorized subsets of servers are able to compute the function. A user who wants to compute f(x) should send x to the members of an authorized subset and receive information which enables him to compute f(x). We require that such a scheme is consistent, i.e. that given an input x all authorized subsets compute the same value f(x). The solutions we present enable the operation of many servers, prevent- ing bottlenecks or single points of failure. There are also no single entities which can compromise the security of the entire network. The solutions can be used to distribute the operation of a Key Distribution Center (KDC). They are far better than the known partitioning to domains or replication solutions to this problem, and are especially suited to handle users of multicast groups.

TITLE : Cipher text policy Attribute based Encryption with anonymous access policy
AUTHOR : A.Balu, K.Kuppusamy
YEAR : 2013
DESCRIPTION :

In Cipher text Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the cipher text. We propose a method in which the access policy need not be sent along with the cipher text, by which we are able to preserve the privacy of the encryptor. The proposed construction is provably secure under Decision Bilinear Diffe-Hellman assumption.

TITLE :Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data
AUTHOR : Jan Camenisch, Markulf Kohlweiss, Alfredo Rial, and Caroline Sheedy
YEAR : 2011
DESCRIPTION :

Searchable encryption schemes provide an important mechanism to cryptographically protect data while keeping it available to be searched and accessed. In a common approach for their construction, the encrypting entity chooses one or several keywords that describe the content of each encrypted record of data. To perform a search, a user obtains a trapdoor for a keyword of her interest and uses this trapdoor to find all the data described by this keyword. We present a searchable encryption scheme that allows users to privately search by keywords on encrypted data in a public key setting and decrypt the search results. To this end, we define and implement two primitives: public key encryption with oblivious keyword search (PEOKS) and committed blind anonymous identity-based encryption (IBE). PEOKS is an extension of public key encryption with keyword search (PEKS) in which users can obtain trapdoors from the secret key holder without revealing the keywords. Furthermore, we define committed blind trapdoor extraction, which facilitates the definition of authorisation policies to describe which trapdoor a particular user can request. We construct a PEOKS scheme by using our other primitive, which we believe to be

the first blind and anonymous IBE scheme. We apply our PEOKS scheme to build a public key encrypted database that permits authorised private searches, i.e., neither the keywords nor the search results are revealed.

TITLE :Short Signatures Without Random Oracles
AUTHOR : Dan Boneh, Xavier Boyen
YEAR : 2009
DESCRIPTION :

We describe a short signature scheme which is existentially unforgeable under a chosen message attack without using random oracles. The security of our scheme depends on a new complexity assumption we call the Strong Diffie-Hellman assumption. This assumption has similar properties to the Strong RSA assumption, hence the name. Strong RSA was previously used to construct signature schemes without random oracles. However, signatures generated by our scheme are much shorter and simpler than signatures from schemes based on Strong RSA. Furthermore, our scheme provides a limited form of message recovery.

TITLE :Efficient Protocols for Set Membership andRange Proofs
AUTHOR : Jan Camenisch, Rafik Chaabouni1, and abhi shelat
YEAR : 2012
DESCRIPTION :

We consider the following problem: Given a commitment to a value σ, prove in zero-knowledge that σ belongs to some discrete set Φ. The set Φ can perhaps be a list of cities or clubs; often Φ can be a numerical range such as [1, 220]. This problem arises in e-cash systems, anonymous credential systems, and various other practical uses of zero-knowledge protocols. When using commitment schemes relying on RSA-like assumptions, there are solutions to this problem which require only a constant number of RSA-group elements to be exchanged between the prover and verifier.

TITLE : Fully Secure Multi-authority Cipher text-PolicyAttribute-Based Encryption without Random Oracles
AUTHOR : Zhen Liu, Zhenfu Cao, Qiong Huang, and Duncan S. Wong,and Tsz Hon Yuen
YEAR : 2014
DESCRIPTION :

Recently Lewko and Waters proposed the first fully secure multi-authority ciphertext-policy attribute-based encryption (CP-ABE) system in the random oracle model, and leave the construction of a fully secure multi-authority CP-ABE in the standard model as an open problem. Also, there is no CP-ABE system which can completely prevent individual authorities from decrypting ciphertexts. In this paper, we propose a new multi-authority CP-ABE system which addresses these two problems positively. In this new system, there are multiple Central Authorities (CAs) and Attribute Authorities (AAs), the CAs issue identity-related keys to users and are not involved in any attribute related operations, AAs issue attribute-related keys to users and each AA manages a different domain of attributes. The AAs operate independently from each other and do not need to know the existence of other AAs. Messages can be encrypted under any monotone access structure over the entire attribute universe. The system is adaptively secure in the standard model with adaptive authority corruption, and can support large attribute universe.

TITLE : On the Practical Security of Inner Product Functional Encryption
AUTHOR : Shashank Agrawal,Shweta Agrawal,Saikrishna Badrinarayanan,Abishek Kumarasubramanian ,Manoj Prabhakaran,Amit Sahai.
YEAR : 2010
DESCRIPTION :

Functional Encryption (FE) is an exciting new paradigm that extends the notion of public key encryption. In this work we explore the security of Inner Product Functional Encryption schemes with the goal of achieving the highest security against practically feasible attacks. While there has been substantial research effort in defining meaningful security models for FE, known definitions run into one of the following difficulties – if general and strong, the definition can be shown impossible to achieve, whereas achievable definitions necessarily restrict the usage scenarios in which FE schemes can be deployed. We argue that it is extremely hard to control the nature of usage scenarios that may arise in practice. Any cryptographic scheme may be deployed in an arbitrarily complex environment and it is vital to have meaningful security guarantees for general scenarios. Hence, in this work, we examine whether it is possible to analyze the security of FE in a wider variety of usage scenarios, but with respect to a meaningful class of adversarial attacks known to be possible in practice. Note that known impossibilities necessitate that we must either restrict the usage scenarios (as done in previous works), or the class of attacks (this work). We study real world loss-of-secrecy attacks against Functional Encryption for Inner Product predicates constructed over elliptic curve groups.

TITLE :Privacy-Preserving Decentralized Key PolicyAttribute-Based Encryption
AUTHOR : Girija Patil
YEAR : 2015

DESCRIPTION :

In Attribute-based Encryption (ABE) scheme, attributes play a crucial role. Attributes have been utilized to generate a public key for encrypting data and have been used as an access policy to control users' access. The access policy can be divided as either key-policy or cipher text-policy. The key-policy is the access structure on the user's private key, and the cipher text-policy is the access structure on the cipher text. And the access structure can also be further divided as either monotonic or non-monotonic one. Using ABE schemes one can have the Advantages:

(1) To reduce the communication overhead of the Internet, and

(2) To provide fine-grained access control.

III. EXISTING SYSTEM

In existing, they have focused on predicting reliability of various factors involved in building enterprise application, nonetheless, considered reliability of remote web service as constants For remote web services the vender will provide probabilistic details about the flow of executing user requests

3.1 DISADVANTAGE

- Quality of Service is not good.
- Response time calculation is not possible.

IV. PROPOSED SYSTEM

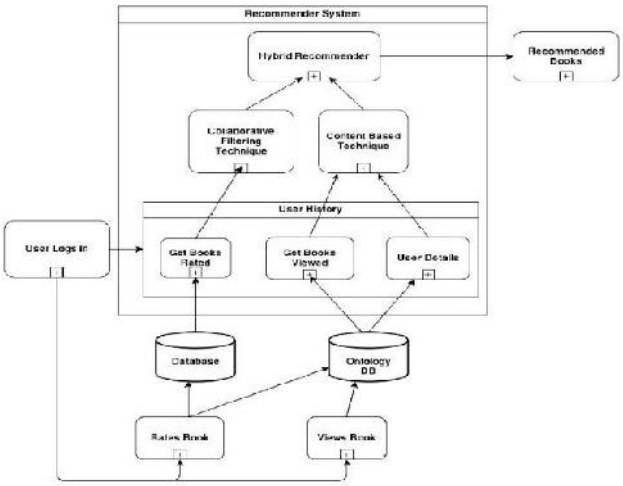
In this paper, We propose a novel method for Quos metrification based on Hidden Markov Models (HMM), which further suggests an optimal path for the execution of user requests. The users can weigh their options directly and individually, for themselves.Models (HMM), which further suggests an optimal path for the execution of user requests. The technique we show can be used to measure and predict the behavior of Web Services in terms of response time, and can thus be used to rank services quantitatively rather than just qualitatively..

4.1 ADVANTAGES

- Quality of Service is good.
- Response time calculation is possible.

V. SYSTEM ARCHITECTURE

A system architecture is the visual representation conceptual model that defines the behavior, structure and more views of a system. An architecture description is a formal explanation and representation of an architecture, organized in a way that supports reasoning about the behaviors and structure of the system



VI. ALGORITHM

6.1 KMEANS CLUSTER:

1. It allows us to cluster the data into different groups and a convenient way to discover the categories ofgroups in the unlabeled dataset on its own without the need for any training.
2. It is a centroid-based algorithm, where each cluster is associated with a centroid. The main aim of this algorithm is to minimize the sum of distances between the data point and their corresponding clusters.

The algorithm takes the unlabeled dataset as input, divides the dataset into k-number of clusters, and repeats the process until it does not find the best clusters. The value of k should be predetermined in this algorithm.

The k-means clustering algorithm mainly performs two tasks:

- Determines the best value for K center points or centroids by an iterative process.
- Assigns each data point to its closest k-center. Those data points which are near to the particular k-center create a cluster.

6.2 LINEAR REGRESSION

- Linear Regression is a machine learning algorithm based on supervised learning. It performs a regression task. Regression models a target prediction value based on independent variables. It is mostly used for finding out the relationship between variables and forecasting. Different

regression models differ based on – the kind of relationship between dependent and independent variables they are considering, and the number of independent variables getting used.

- Linear regression performs the task to predict a dependent variable value (y) based on a given independent variable (x). So, this regression technique finds out a linear relationship between x (input) and y(output). Hence, the name is Linear Regression.
  In the figure above, X (input) is the work experience and Y (output) is the salary of a person. The regression line is the best fit line for our model.

6.3 TENSORFLOW

- TensorFlow Recommenders (TFRS) is a library for building recommender system models.
- It helps with the full workflow of building a recommender system: data preparation, model formulation, training, evaluation, and deployment.
- It's built on Keras and aims to have a gentle learning curve while still giving you the flexibility to build complex models.

TFRS makes it possible to:

- Build and evaluate flexible recommendation retrieval models.
- Freely incorporate item, user, and context information into recommendation models
- Train multi-task models that jointly optimize multiple recommendation objectives.

VII. LIST OF MODULES

7.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. . Logging in is usually used to enter a specific page.

7.2 Order Process

Once you login there is book list page. What the book you like and comfortable with price also means click buy now. After you have to once again see the title of what the you have to be purchased and click make payment option it will go for bank login page

7.3Payment Process

Once you click make payment option there is bank login page. You have to enter your account number, username and password then only they can able to connect the server. There is transfer account option just enter your account number and transfer account number and enter the amount click submit button the enter amount will be updated in to owner account.

7.4 Owner View

There is a separate login for owner once login the owner and click the book request page. There is the detail of whom to buy and which book to be buy and also having the user detail. Once he paid the amount means click choose file option and upload the book click submit button in that book will send only for particular user.

7.4.1User Download

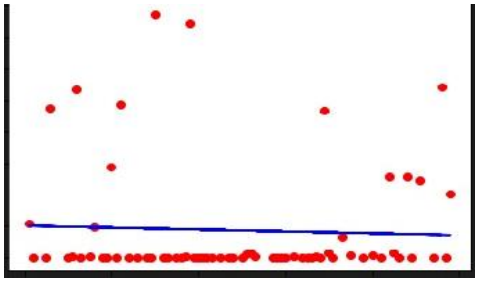
Once owner accept the request and send file means user to be login them account. To connect with server user must give their username and password then only they can able to connect the server. See the page and select the download option your will get the file for what you have to be ordered.

VIII. DATASET

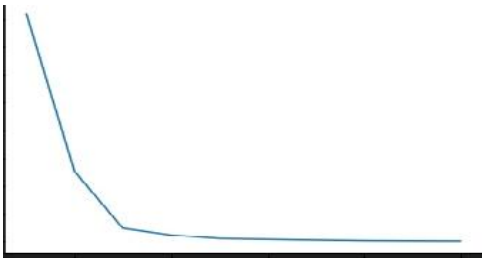
id	book_id	best_book_id	work_id	books_co	isbn	isbn13	authors	original_p	original_t	title	language_	average_r
id	2767052	2767052	2792775	272	439023483	9.78E+12	Suzanne C	2008	The Hung	The Hunge	eng	4.34
id	3	3	4640799	491	439554934	9.78E+12	J.K. Rowli	1997	Harry Pott	Harry Pott	eng	4.44
id	41865	41865	3212258	226	316015849	9.78E+12	Stephenie	2005	Twilight	Twilight (Tw	en-US	3.57
id	2657	2657	3275794	487	61120081	9.78E+12	Harper Le	1960	To Kill a M	To Kill a M	eng	4.25

IX. EXPERIMENT ANALYSIS

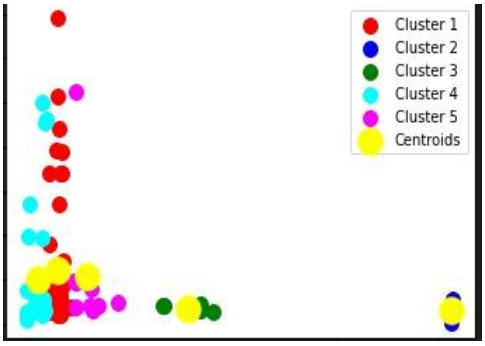
KMEANS CLUSTER:



LINEAR REGRESSION:



TENSORFLOW:



X. CONCLUSION

In this paper, we consider the problem of verifying the utility of data released by non-interactive differentially private methods. Similar mechanisms are proposed to achieve the goal for set-valued and relational data respectively. The proposed solutions require the publisher to provide auxiliary datasets in cipher text along with the publishing data. The providers then sequentially verify the auxiliary datasets to see whether their data is correctly involved. And finally, any individual can compute a linear transformation of the utility of the released dataset in cipher text with those verified auxiliary datasets and verify whether the utility can be accepted. Experiments illustrate the efficiency of the solution which is mainly affected by the number of providers and the size of the data.

XI. ACKNOWLEDGEMENT

The authors would like to thank Mrs. UMARANI Cfor her suggestions and excellent guidance throughout the project period.

REFERENCES

[1] Dima Alhadidi, Noman Mohammed, Benjamin C. M. Fung, and Mourad Debbabi. Secure distributed framework for achieving ϵ- differential privacy. In Privacy Enhancing Technologies, volume 7384 of LNCS, pages 120–139, 2012.

[2] Gilles Barthe, Boris K¨opf, Federico Olmedo, and Santiago Zanella B´eguelin. Probabilistic relational reasoning for differential privacy. ACM SIGPLAN Notices, 47(1):97–110, 2012.

[3] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In Theory of cryptography, pages 325–341. Springer, 2005.

[4] Rui Chen, Benjamin Fung, and Bipin C Desai. Differentially private trajectory data publication. arXiv preprint arXiv:1112.2020, 2011.

[5] Rui Chen, Benjamin Fung, Bipin C. Desai, and N´eriah M. Sossou. Differentially private transit data publication: A case study on the montreal transportation system. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'12), pages 213–221, 2012.

[6] Rui Chen, Noman Mohammed, Benjamin C. M. Fung, Bipin C. Desai, and Li Xiong. Publishing set-valued data via differential privacy. Proceedings of the VLDB Endowment, 4(11):1087–1098, 2011.

[7] Cynthia Dwork. Differential privacy. In Automata, languages and programming, pages 1–12. 2006.

[8] Cynthia Dwork. Differential privacy: A survey of results. In Theory and Applications of Models of Computation, pages 1–19. 2008.

[9] Cynthia Dwork. Differential privacy in new settings. In Proceedings of the 21st annual ACM-SIAM symposium on Discrete Algorithms (SODA'10), pages 174–183, 2010.

[10] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography, pages 265–284. 2006.

[11] Liyue Fan, Li Xiong, and Vaidy Sunderam. FAST: differentially private real-time aggregate monitor with filtering and adaptive sampling. In Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data (SIGMOD'13), pages 1065–1068, 2013.

[12] David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), pages 44–61, 2010.

[13] Benjamin Fung, Ke Wang, Rui Chen, and Philip S. Yu. Privacypreserving data publishing: A survey of recent developments. ACM Computing Surveys (CSUR), 42(4):14, 2010.

[14] Yuan Hong, Jaideep Vaidya, Haibing Lu, Panagiotis Karras, and Sanjay Goel. Collaborative search log sanitization: toward differential privacy and boosted utility. Dependable and Secure Computing, IEEE Transactions on, 12(5):504–518, 2015.

[15] Wei Jiang and Chris Clifton. A secure distributed framework for achieving k-anonymity. The International Journal on Very Large Data Bases, 15(4):316–333, 2006.

[16] Jaewoo Lee and Chris Clifton. How much is enough? choosing ε for differential privacy. In Information Security, pages 325–340. 2011.

[17] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. tcloseness: Privacy beyond k-anonymity and l-diversity. In Proceedings of the 23rd International Conference on Data Engineering (ICDE'07), pages 106–115, 2007.

[18] Junqiang Liu and Ke Wang. Enforcing vocabulary k-anonymity by semantic similarity based clustering. In Proceedings of the 10th International Conference on Data Mining (ICDM'10), pages 899–904. IEEE, 2010.

[19] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.

[20] Frank McSherry and Ratul Mahajan. Differentially-private network trace analysis. ACM SIGCOMM Computer Communication Review, 41(4):123–134, 2011.

[21] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07), pages 94–103, 2007.

[22] Nabeel Mohammed, Dima Alhadidi, Benjamin Fung, and Mourad Debbabi. Secure two-party differentially private data release for vertically partitioned data. Dependable and Secure Computing, IEEE Transactions on, 11(1):59–71, 2014.

[23] Noman Mohammed. Models and Algorithms for Private Data Sharing. PhD thesis, Concordia University, 2012.

[24] Noman Mohammed, Rui Chen, Benjamin Fung, and Philip S. Yu. Differentially private data release for data mining. In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'11), pages 493–501, 2011.

[25] Noman Mohammed, Benjamin Fung, Patrick CK Hung, and Cheuk-Kwong Lee. Centralized and distributed anonymization for high-dimensional healthcare data. ACM Transactions on Knowledge Discovery from Data (TKDD), 4(4):18, 2010.

[26] Shangfu Peng, Yin Yang, Zhenjie Zhang, Marianne Winslett, and Yong Yu. Query optimization for differentially private data management systems. In Proceedings of the 29th International Conference on Data Engineering (ICDE'13), pages 1093–1104, 2013.

[27] Wahbeh Qardaji, Weining Yang, and Ninghui Li. Differentially private grids for geospatial data. In Proceedings of the 29th International Conference on Data Engineering (ICDE'13), pages 757–768, 2013.

[28] Entong Shen and Ting Yu. Mining frequent graph patterns with differential privacy. In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, pages 545–553. ACM, 2013.

[29] Elaine Shi, T-H. Hubert Chan, Eleanor G. Rieffel, Richard Chow, and Dawn Song. Privacy-preserving aggregation of time-series data. In Proceedings of the 18th Network and Distributed System Security Symposium (NDSS'11), 2011.

[30] Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570, 2002.

[31] Michael Carl Tschantz, Dilsun Kaynar, and Annular Datta. Formal verification of differential privacy for interactive systems. Electronic Notes in Theoretical Computer Science, 276:61–79, 2011.

[32] [32] Shelley Wood. Diovan data-manipulation scandal touches novartis in japan. http://www.medscape.com/viewarticle/808152. Accessed July 30, 2014.

[33] Xiaokui Xiao, Guozhang Wang, and Johannes Gehrke. Differential privacy via wavelet transforms. IEEE Transactions on Knowledge and Data Engineering,, 23(8):1200–1214, 2011.

[34]]Jia Xu, Zhenjie Zhang, Xiaokui Xiao, Yin Yang, Ge Yu, and Marianne Winslett. Differentially private histogram publication. The VLDB Journal, 22(6):797–822, 2013.

[35] Jian Xu, Wei Wang, Jian Pei, Xiaoyuan Wang, Baile Shi, and Ada Wai-Chee Fu. Utility-based anonymization for privacy preservation with less information loss. ACM SIGKDD Explorations Newsletter, 8(2):21–30, 2006.

[36] Grigory Yaroslavtsev, G. Cormode, C. M. Procopiuc, and D. Srivastava. Accurate and efficient private release of datacubes and contingency tables. In Proceedings of the

29th International Conference on Data Engineering (ICDE'13), pages 745–756, 2013.

[37] Ganzhao Yuan, Zhenjie Zhang, Marianne Winslett, Xiaokui Xiao, Yin Yang, and Zhifeng Hao. Low-rank mechanism: optimizing batch queries under differential privacy. Proceedings of the VLDB Endowment, 5(11):1352–1363, 2012.

[38] Xiaojian Zhang, Xiaofeng Meng, and Rui Chen. Differentially private set-valued data release against incremental updates. In Database Systems for Advanced Applications, pages 392–406, 2013.

[39] Zijian Zheng, Ron Kohavi, and Llew Mason. Real world performance of association rule algorithms. In Proceedings of the 7th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'01), pages 401–406. ACM, 2001.

[40] Sheng Zhong, Zhiqiang Yang, and Rebecca N Wright. Privacyenhancing k-anonymization of customer data. In Proceedings of the 24th ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, pages 139–147. ACM, 2005.