E-COMMERCE WEBSITE USING SKYLINE QUERIES

N R Vishnu Priya [1], Emayal R M[2], Little Libisha A[3]

[1]Assistant Professor, Department of Information Technology, Jeppiaar SRR Engineering College, Chennai
[2,3]Students, Department of Information Technology, Jeppiaar SRR Engineering College, Chennai.

---***---

Abstract – *In these modern days every one prefer online shopping .The main problem faced by customers are unaffordable price, cannot BG directly etc., The website provide the details about the products and offers on products to user .User can buy and even bargain through e-commerce website. The Pre -processing on data can be performed by admin to send to web server. User can easily buy the product through websites which is efficient on big data broadcasting. The SQL data's are also used in banking process and further pave way for payment .The skl quries are main component for the pre-processing.*

Key Words: **Bargain (BG), SkyLine Queries(SKL)**

1. INTRODUCTION

The main aim of this paper is to study the problem of secure skyline queries over encrypted data. The skyline query is particularly important for multi-criteria decision making but also presents significant challenges due to its complex computations. The emerging computing paradigm, cloud computing attracts increasing attention from both research and industry communities. Outsourcing data and computation to cloud server provides a cost effective way to support large scale data storage and query processing. However, due to security and privacy concerns, sensitive data need to be protected from the cloud server as well as other unauthorized users. In this paper we focus on the problem of secure skyline queries on encrypted data, another type of similarity search important for multi-criteria decision making. The skyline or Pareto of a multi-dimensional dataset given a query point consists of the data points that are not dominated by other points. A data point dominates another if it is closer to the query point in at least one dimension and at least as close to the query point in every other dimension. The skyline query is particularly useful for selecting similar (or best) records when a single aggregated distance metric with all dimensions is hard to define.

2. RELATED WORKS

Shai Halevi[1]: Victor Should Gentry's bootstrapping technique is still the only known method of obtaining fully homomorphic ncryption where the system's parameters do not depend on the complexity of the evaluated functions. Bootstrapping involves a decryption procedure where the scheme's decryption algorithm is evaluated homomorphically. Prior to this work there were very few implementations of recryption, and fewer still that can handle \packed ciphertexts" that encrypt vectors of elements. In the current work, we report on an implementation of recryption of fully-packed ciphertexts using the HElib library for somewhat-homomorphic encryption. This implementation required extending previous recryption algorithms from the literature, as well as many aspects of the HElib library. Our implementation supports bootstrapping of packed ciphertexts over many extension _elds/rings. One example that we tested involves ciphertexts that encrypt vectors of 1024 elements from GF(216). In that setting, the recryption procedure takes under 3 minutes (at security-level _ 80) on a single core, and allows a multiplicative depth-11 computation before the next recryption is needed. This report updates the results that we reported in Eurocrypt 2015 in several ways. Most importantly, it includes a much more robust method for deriving the parameters, ensuring that recryption errors only occur with negligible probability. Many aspects of this analysis are proven, and for the few well-speci_fied heuristics that we made, we report on thorough experimentation to validate them. The procedure that we describe here is also signi_cantly more effi_cient than in the previous version, incorporating many optimizations that were reported elsewhere (such as more effi_cient linear transformations) and adding a few new ones. Finally, our implementation now also incorporates Chen and Han's techniques from Eurocrypt 2018 for more effi_cient digit extraction (for some parameters), as well as for \thin bootstrapping" when the ciphertext is only sparsely packed.

Long Chen1,2 and Zhenfeng Zhang [2]: Despite a great deal of progress in recent years, efficiency of fully homomorphic encryption (FHE) is still a major concern. Specifically, the bootstrapping procedure is the most costly part of a FHE scheme. FHE schemes with ring element plaintexts, such as the ring-LWE based BGV scheme, are the most efficient ones, since they can not only encrypt a ring element instead of a single bit in one ciphertext, but also support CRT-based ciphertext packing techniques. Thanks to homomorphic operations in a SIMD fashion (Single Instruction Multiple Data), the ring-LWE BGV scheme can achieve a nearly optimal homomorphic evaluation. However, the BGV scheme, as implemented in HElib, can only bootstrap within super-polynomial noise so far. Note that such a noise rate for a ring-LWE based scheme is less safe and more costly, because one has to choose larger dimensions to ensure security. On the other hand, existing polynomial noise bootstrapping techniques can only be applied to FHE schemes with bit plaintexts. In this paper, we provid plaintexts. Specifically, our bootstrapping method allows users to choose any plaintext modulus $p > 1$ and any modulus polynomial $\Phi(X)$ for the BGV scheme. Our bootstrapping method incurs only polynomial error O(n3) ·B for lattice dimension n and noise bound B comparing to (B · poly(n)) ˜O (log(n)) for previous best methods. Concretely, to achieve 70 bit security, the dimension of the lattice that we use is no more than 212, while previous methods in HElib need about 214 to 2

Manish Kesarwani, Akshar Kaul, Prasad Naldurg[3]:Enterprise customers of cloud services are wary of outsourcing sensitive user and business data due to inherent security and privacy concerns. In this context, storing and computing directly on encrypted data is an attractive solution, especially against insider attacks. Homomorphic encryption, the keystone enabling technology is unfortunately prohibitively expensive. In this paper, we focus on finding k-Nearest Neighbours (k-NN) directly on encrypted data, a basic data-mining and machine learning algorithm.

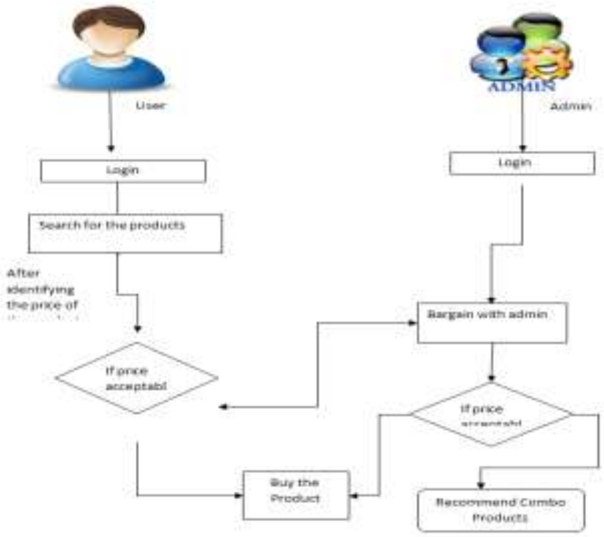
Wenhui Yu, Zheng Qin, Jinfei Liu[4]:Skyline, aiming at €nding a Pareto optimal subset of points in a multi-dimensional dataset, has gained great interest due to its extensive use for multi-criteria analysis and decision making. Skyline consists of all points that are not dominated by, or not worse than other points. It is a candidate set of optimal solution, which depends on a speci€c evaluation criterion for optimum. However, conventional skyline queries, which return individual points, are inadequate in group querying case since optimal combinations are required. To address this gap, we study the skyline computation in group case and propose fast methods to €nd the group-based skyline (G-skyline), which contains Pareto optimal groups. For computing the front k skyline layers, we lay out an efficient approach that does the search concurrently on each dimension and investigates each point in subspace. A.er that, we present a novel structure to construct the G-skyline with a queue of combinations of the €rst-layer points. Experimental results show that our algorithms are several orders of magnitude faster than the previous work.

Twaha Ahmadi Fuko[5]:Intel SGX provides, record level, secure hardware enabled execution environment for program and data to ensure its confidentiality and integrity. However, this work focuses mainly on memory management aspect of Intel SGX. It is an attempt to explain how Intel SGX implements hardware control structures such as virtual memory, data structures, address translation, translation look-aside buffer (TLB), memory management techniques and how it puts processor's memory management unit in action.

3. PROPOSED SYSTEM

In the proposed system, there is bit of communication between the data owner and user about the price of the product. We are using skyline queries on big data broadcasting to display the prioritized products. By using preprocessing we are converting the uncategorized file into categorized file and update into webserver. Also , the big data broadcasting is used to compare the servers and display the data using skyline queries .And finally the combo offers with item based recommendation are also done . We used a completely secure skyline protocol on encrypted data using skyline queries. It ensures semantic security therein the cloud server knows nothing about the data including indirect data patterns, query, also because the query result. Additionally, the client and data owner don't need to participate within the computation.

4. PROPOSED ARCHITECTURE



5. METHODOLOGY

5.1 SECURE SKYLINE PROTOCOL

In the section, we propose a basic secure skyline protocol and show why such an easy solution isn't secure. Then we propose a fully secure skyline protocol. skyline query q, it's like compute the skyline during a transformed space with the query point q because the origin and therefore the absolute distances to q as mapping functions. Hence we first show a preprocessing which maps the dataset to the new space. Since the skyline only depends on the order of the attribute values, we use (pi[j] − q[j])2 which is simpler to compute than |pi[j] − q[j]| because the mapping function.

5.2 DYNAMIC SKYLINE QUERY

Skyline Definitions Definition dimensional pis are P, a[j] the we those ≤ jsay th 1. pbdimension points [j], (Skyline). pa space. dominates which for Let of are Given at ppleast i pnot a band , and a denoted dominated one 1 dataset p≤ b j, be j p≤ aby [j] two P m. by p= < a the various any p≺ {pb[j], p1skyline , other b...,p, points n} in m- in if for all j, where points pi[j] .

Mapped data = q |pin i[j]−q[j]|+q[j]. The space, original and space.

5.3 FULLY SECURED PROTOCOL

The data is secure and properly selects the skyline tuple if there's just one minimum. To address this, we employ order-preserving perturbation which adds a set of mutually different bit sequence to a set of values such that: 1) if the original values are equal to each other, the perturbed values are guaranteed not equal to each other, and 2) if the original values are not equal to each other, their order is preserved. Concretely, given n numbers in their binary representations, we add a [logn]-bit sequence to the end of each Epk(S(ti)), each represents a unique bit sequence in the range of [0,n − 1]. This way, the perturbed values are guaranteed to be different from each other while their order is preserved since the added bits are the least significant bits. Line 10 of Algorithm 5 shows this step. We note that we can multiply each sum Epk(S(ti)) by n and uniquely add a value from [0,n − 1] to each Epk(S(ti)), hence guarantee they are not equal to each other.

6. MODULE DESCRIPTION

A common approach to guard the confidentiality of outsourced data is to encrypt the info . to guard the confidentiality of the query from cloud authorized clients also send encrypted queries to the cloud server. Figure 1 illustrates our problem scenario of secure query processing over encrypted data within the cloud. The info owner outsources encrypted data to the cloud server. The cloud server handles the queries of client on the encrypted data and returns the query result to the client. During the query processing, the cloud server shouldn't gain any knowledge about the info, data patterns, query, and query result.

6.1 Admin and User Authentication

User has an initial level Registration Process at the online end. The users have to provide required information for process. The server successively stores the knowledge in its database, then by using the registered information the user can login by their respective credentials which they created during the registration process. of these process avail for the admin also.

6.2 Search for the products

In this module the user can see the n number of products as their wish and they can view the reviews and ratings of the particular product .If the user wants to buy the product they can search the product with their respective name and the key word. It shows a lot of options for you to choose and select the quality product by using the rating and review which is given by the other users and also it shows the most relevant product at the top.

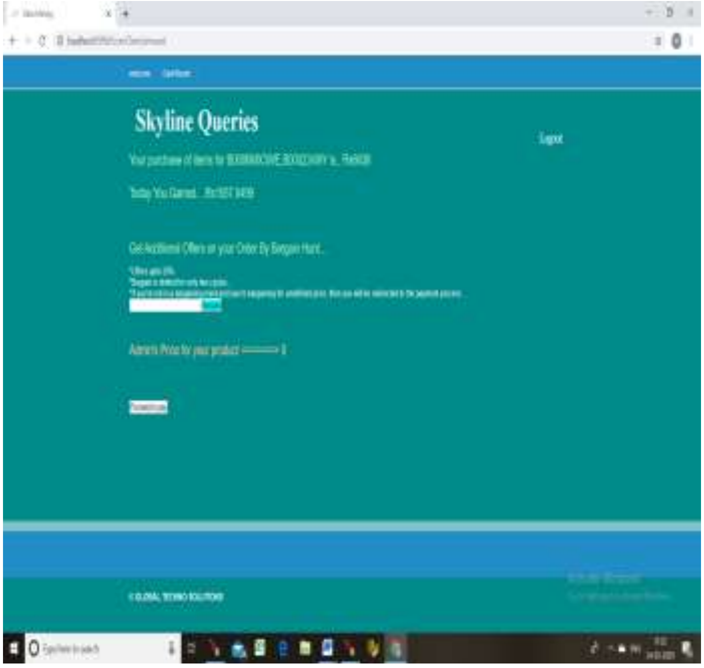
6.3 Bargain with the Admin

In this module after you select the products and identifying the price if the user is not satisfied with price given by the respective sellers they can bargain them and you can suggest the price which you want to buy and if the admin is accepted your request you can buy this product with the satisfaction and if he is willing to the price he can able reject proposal which was given by you.

6.4 Suggest Related Products with Offers

In this module after ready to buy the product with the above advantages you will get the relevant products which you wanted to buy and it comes with offer which is easy and simple way to buy the product. The combo offer will be recommended.

7. RESULT



Skyline Queries

Logout

Your purchase of items for [illegible] is [illegible]

Today You Gained [illegible]

Get Additional Offers on your Order By Bargain Hunt..

[illegible]

Admin's Price for your product ——> 0

Therefore, by using these algorithms and technologies we can buy products through e-commerce website by using the latest technique on skyline queries.

8. CONCLUSION

This processes are secure and efficient in these modern days. This process is mainly time consuming. Cloud computing attracts increasing attention from both research and industry communities. Outsourcing data and computation to cloud server provides a price effective thanks to support large scale data storage and query processing. However, due to security and privacy concerns, sensitive data need to be protected from the cloud server as well as other unauthorized users. We present a set of secure sub protocols for computing basic functions on encrypted data that will be used to construct our secure skyline query protocol. We have also designed a parallel framework for effective reducing computation time together with the two optimizations, data partitioning and lazy merging.

9. FUTURE ENHANCEMENTS

In the proposed system, there is bit of communication between the data owner and user about the price of the product. We are using skyline queries on big data broadcasting to display the prioritized products. By using preprocessing we are converting the uncategorized file into categorized file and update into webserver. Also , the big data broadcasting is used to compare the servers and display the data using skyline queries .And finally the combo offers with item based recommendation are also done .

REFERENCES

[1] F. Baldimtsi and O. Ohrimenko. Sorting and searching behind the curtain. In FC 2015, pages 127–146, 2015.
[2] A. Beimel. Secret-sharing schemes: a survey. In International Conference on Coding and Cryptology, pages 11–46. Springer, 2011.
[3] J.L. Bentley. Multidimensional divide-and-conquer. Commun. ACM, 23(4):214–229, 1980.
[4] J. L. Bentley, H. T. Kung, M. Schkolnick, and C. D. Thompson. On the average number of maxima in a set of vectors and applications. J. ACM, 25(4):536–543, 1978.
[5] S. B¨orzs¨onyi, D. Kossmann, and K. Stocker. The skyline operator. In ICDE 2001.
[6] S. Bothe, A. Cuzzocrea, P. Karras, and A. Vlachou. Skyline query processing over encrypted data: An attribute-order-preserving-free approach. In PSBD@CIKM, pages 37–43, 2014.
[7] S. Bothe, P. Karras, and A. Vlachou. eskyline: Processing skyline queries over encrypted data. PVLDB, 6(12):1338–1341, 2013.
[8] C. Y. Chan, H. V. Jagadish, K.-L. Tan, A. K. H. Tung, and Z. Zhang. Finding k-dominant skylines in high dimensional space. In SIGMOD Conference, pages 503–514, 2006.
[9] W. Chen, M. Liu, R. Zhang, Y. Zhang, and S. Liu. Secure outsourced skyline query processing via un trusted cloud service providers. In INFOCOM 2016.
[10] V. Costan and S. Devadas. Intel sgx explained. Technical report, Cryptology ePrint Archive, Report 2016/086, 20 16. http://eprint. iacr. org.