International Conference on Recent Innovations in Science and Engineering
Buddha Institute of Technology, Gida, Gorakhpur (India) (ICRISE-18)
1st-2nd April 2018 www.conferenceworld.in ISBN : 978-93-87793-15-6

A Literature Survey on Order Preserving Encryption

Nivedita W. Wasankar[1], A.V. Deorankar[2]

[1]*M. Tech. Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) (India)*

[2]*Assistant Professor, Department Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) (India)*

ABSTRACT

The growing industry of cloud gives a service paradigm of storage/computation outsourcing. It helps to reduce users' burden of IT infrastructure maintenance and also reduce the cost for both the enterprises and individual users. It would be necessary to encrypt critical data before hosting to third-parity, but in the meantime, the database should be capable to process queries on encrypted data. Many research works have been done to support processing of search query on encrypted data that also include the order preserving encryption (OPE) schemes. Order-preserving encryption (OPE) permits encrypting data without losing information of the order relation among the encrypted data items. So, the execution of compare, order and grouping query operations can be processedlike on plaintext data. It allows databases to do range queries over encrypted data. This is a useful featurespecially for cloud databases which mostly run in untrusted environments. Several OPE schemes has been proposed in the last few years, but that are unable touse in real world scenarios.In this paper, the literature survey of OPE is given.

Keyword:Cloud database, Encrypted data,Outsourcing, Order-preserving encryption (OPE), Range queries.

I.INTRODUCTION

Order-preserving symmetric encryption (OPE) is a deterministic encryption scheme whose encryptionfunction preserves numerical ordering of the plaintexts. This means that comparing encrypted data returns the same result than comparing the original data. This permits to order encrypted data without the need of decryption. This cryptosystem is useful in databases, in which record fields are encrypted because it permits to range queries. It is difficult todeterminethat how good a particular order preserving encryption scheme is. In fact, characteristics of order preserving cryptosystems make traditional security analysis useless.

Order-preserving encryption scheme (OPES) permitscomparison operations to be directly applied onencrypted data, without decrypting the operands. Thus, equality and range queries as well as the MAX, MIN, and COUNT queries can be directly processed overencrypted data. Similarly, GROUP BY and ORDER BY operations can also be applied. Only when applying SUM or AVG to a group do the values need to bedecrypted.

OPES is also endowed with the following properties [14]:

1.1. The results of query processing over data encrypted using OPES are exact. They neither contain any false positives nor miss any answer tuple.

1.2. OPES handles updates gracefully. A value in a column can be modified or a new value can be inserted in a column without requiring changes in the encryption of other values.

1.3. OPES can easily be integrated with existing database systems as it has been designed to work with the existing indexing structures such as Btrees. The fact that the database is encrypted can be made transparent to the applications.

II.LITRATURE SURVEY

In 2004, R. Agrawal et al. [1] propose the encryptionof data that belonging to a integers subset [p_{min}, p_{max}],although they suggested that the possibility of treating floatingpoint values as if they were integers, sincepositives maintain the same order, and for the negatives,that have the order reversed, only need tosubtract the resulting integer from the largest negative.In their proposed method, data transforms for follow certain statistical distribution into ciphertexts. It maintains order and follows a different distribution,chosen by the user. To generate the encryptionfunction, they convertall the data to encrypt, the list of distribution samples has to be emulated.The auxiliary information is necessary for the encryptionand decryption of data. It will begenerated from all these samples. To model the distributions, data need to be partitioned inbuckets. Linear interpolation will be used in it.During encrypting, data is first convert in a uniformdistribution and then transformed into the targetdistribution.One of the drawbacks of their propose cryptosystem is key generation. While it is relatively small and its generation is linearto size of the database. After a key generation, if a large amount of data is added to thedatabase, it will be necessary tochoose a new key and re-encrypt the database.

Boldyrevaet al.[2]The cryptography communityprovided first formal security guarantee of order-preserving encryption. Boldyreva et al. introduce notion in distinguish ability under ordered chosen plaintext attack. They also prove that no other stateless scheme can achieve this notion. It settle for an encryption scheme with less security of a random order-preserving function. This scheme requires only to store a key on the client. Then they statethat a random order-preserving function can achieve the security property of window one-wayness [3]. Furthermore, they provide a scheme that achieves IND-OCPA security, but only requires all plaintexts in advance. If all plaintexts are known in advances, their order can be determine.

Teranishi et al.[4] devise a new OPE scheme that is satisfy its own securitymodel. Even if, their algorithm is less efficient, but it is linear in thesize of the message space. Like Boldyreva et al., a plaintext alwaysencrypt to the same ciphertext value.Even they are stateless, they cannot achieve IND-OCPA security.

Khadem et al. [5] propose a scheme that encrypt equal plaintext values to differing values. This scheme is like to Boldyreva et al. in which a plaintext are mapped to a pseudorandom value in a subrange. This scheme on the basis of domain being a set of consecutive integers for decryption. This scheme permits for non-consecutive integers. This scheme supports updates without worrying about overlapping “buckets” as Khadem et al.

Liu et al. [6] addresses frequency of plaintext values by mapping the plaintext value to a value in an extended message space and splitting the message and ciphertext spaces nonlinearly.

In 2009,Lee et al. [7] proposes the Chaotic Order Preserving Encryption (COPE) scheme.COPE[7] hides theorder of the encrypted values by changing the order of buckets in the plaintext domain. It is secure against known plaintext attack. However, COPE can be used just on trusted server where the encryption keys are used

to perform many queries such as join and range queries. The overhead of range queries over encrypted database is much higher than the overhead of range queries over plaintext database. In addition, it uses many keys to change the order of buckets and in some cases that may lead to have duplicated values. Another drawback in COPE is the encryption and decryption cost. That is because of the computation complexity to randomize the buckets and assign the correct order within each bucket.

Dyer et al.[8] present a new, but simple, randomised *order-preserving encryption* (OPE) scheme relies on the *general approximate common divisor problem* (GACDP). This is the first OPE scheme to be based on a computationalhardness primitive, rather than a security game. This scheme needsonly O(1) arithmetic operations for encryption and decryption. This scheme has optimal information leakage under the consideration of uniformlydistributed plaintexts, and this property extends to some nonuniformdistributions.

Eirini Molla et al.[9]introduces the SOPE (Spatially-based Order-PreservingEncryption) model for *d*-dimensional data. Thismodel is inspired and extends the well-known OPE model in*d*-dimensional databases. It supports the safe storageand efficient retrieval of *d*-dimensional data to a remoteuntrusted server by without discovering the data except thespatial order of the data objects. They propose algorithms for constructing the modeland for efficiently processing a popularquery for *d*-dimensional data, like the range query, point query, the *k*-nearest neighbour query, the reverse *k*-nearest neighborquery, the skyline query*etc.*

In 2013, Popa et al.[10] propose a stronger notion of same-time OPE security which allows an adversary to study the orderof elements which is present in an encrypted database at a time. They present an extension of mOPE, called stOPE, thatachieves stronger definition. They present versions of mOPE and stOPE that protect against a malicious server by using Merkle hashing.

Yanguo peng et al.[11]improved OPE in their work, named hOPE. It is proposed to support homomorphic operations over ciphertexts in addition to comparisons. Based on hOPE, AhOPE and PhOPE are designed to support homomorphic addition and product, respectively. hOPE is a general construction which supports arbitrary HE algorithms and achieves consistent security.

Kerschbaum and Schr¨opfer [12] provide the first efficientIND-OCPA secure order-preserving encryption scheme. [12]presents a keyless IND-OCPA OPE scheme for outsourced data. They discard the need for a separate server and store informationlinear in the number of distinct plaintexts. They are able to reduce the probability of mutation tobe negligible. they reduce the number of rounds in theprotocol between client and server. Theirscheme has constant encryption cost in the average case.

Xiao et al.[13]make weakens the security notion of IND-OCPA to INDOLCPA and require the adversary that can learn ciphertexts only for 'nearby' values. They explain the concept of OPE to generalized OPE (GOPE). The ciphertexts of GOPE may not be numbers. By using special comparison algorithms, GOPE able compare the encrypted data without decrypt them.

III.CONCLUSION

Order-preserving encryption scheme (OPES) allows comparison operations to be directly applied on encrypted data, without decrypting the operands. OPE is very secure encryption scheme for the outsourced database and application. This paper presents the basic concept of the order preserving encryption and present the properties

of the order preserving encryption. This paper can be useful for those who are wishing to carry out research in the direction of the order preserving encryption.

REFERANCES

[1] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, andYirong Xu. Order Preserving Encryption for Numeric Data.In *ACM SIGMOD international conference on Managementof data*, pages 563–574, 2004.

[2] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill. Order-Preserving Symmetric Encryption. In *28th AnnualInternational Conference on Advances in Cryptology: TheTheory and Applications of Cryptographic Techniques -EUROCRYPT'09*, pages 224–241, 2009.

[3] Boldyreva, A., Chenette, N., and O'Neill, A. Order-preserving encryption revisited: improved security analysis and alternative solutions. In *Proceedings of the 31st International Conference onAdvances in Cryptology* (2011), CRYPTO.

[4] Teranishi, I., Yung, M., and Malkin, T. Order-preserving encryption secure beyond one-wayness. In *Proceedings of the 20th International Conference on Advances in Cryptology*.

[5] H. Kadhem et al., MV-OPES: Multivalued-Order Preserving Encryption Scheme: A Novel Scheme for Encrypting Integer Value to Many Different Values, In: *IEICE Transactions on Information andSystems* 93.9 (2010), pp. 2520–2533.

[6] Z. Liu et al., New order preserving encryption model for outsourced databases in cloud environments, In: *Journal of Network and Computer Applications* 59 (2016), pp. 198 –207.

[7] S. Lee, T. Park, D. Lee, T. Nam, and S. Kim, Chaoticorder preserving encryption for efficient and secure querieson databases,IEICE Transactions on Information and Systems, vol.92, pp.2207–2217, 2009.

[8] James Dyer, Martin Dyer and Jie Xu,Order-Preserving Encryption Using Approximate Integer Common Divisors,arXiv:1706.00324v3 [cs.CR], Jun 2017.

[9] Eirini Molla,Theodoros Tzouramanis, Stefanos Gritzalis, SOPE: A Spatial Order Preserving Encryption Model for multi-dimensional Data, Hellanicus Institutional Repository, http://hdl.handle.net/11610/12438.

[10] R. A. Popa, F. H. Li, and N. Zeldovich, An ideal-security protocol for order-preserving encoding, IEEE Symposium on Security and Privacy, 2013.

[11] Yanguo PENG, Hui LI, Jiangtao CUI, Junwei ZHANG, Jianfeng MA & Changgen PENG, hOPE: improved order preserving encryption with the power to homomorphic operations of ciphertexts, SCIENCE CHINA Information Sciences, Vol. 60 062101:1–062101:17,doi: 10.1007/s11432-016-0242-7, June 2017.

[12] F. Kerschbaum, A. Schroepfer, Optimal average-complexity ideal-security order-preserving encryption, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 275–286.

[13] L. Xiao, I.-L. Yen, D. Huynh, A note for the ideal orderpreservingencryption object and generalized order-preservingencryption., IACR Cryptology ePrint Archive 2012 (2012) 350.

[14] http://cryptowiki.net/index.php?title=Order-preserving_encryption.