ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Ordered Bucketization Encryption for the Privacy Secure Data

Dr. K. Swathi[1]
Professor and Head
Department of Computer science &Engineering
Cauvery College of Engineering & Technology
Trichy (TN) - India

S. Ramanathan[2]
Scholar
Department of Computer science &Engineering
Cauvery College of Engineering & Technology
Trichy (TN) - India

R. Vijayanathan[3]
Senior Librarian and Head
Department of Library and Information Science
Cauvery College of Engineering & Technology
Trichy (TN) - India

Abstract: ***The security for data in the ordered bucketization (OB) as a cryptographic object. In OB, plaintext space is divided into p disjoint buckets, numbered from 1 to p, based on the order of the ranges that they cover. With bucketization, including OB, various types of SQL queries over encrypted data are possible, if the bucket number, which corresponds to the original plaintext before encryption, is attached to each encrypted data. Therefore, this method is very useful when users cannot store their data without encryption such as in a cloud computing environment. Due to lack in data security OB can be a replacement for an order preserving encryption (OPE). That also not provides security instead of removing False Positive. This paper defines new symmetric encryption scheme with OB (EOB) that can be constructed with any OB scheme is defined. In EOB, the result of encryption is in the form of bucket#||ciphertext, where bucket# refers to the bucket number of messages that are encrypted; and the bucket number is the result of OB, and the ciphertext part is the result of the conventional symmetric encryption. And also implement the bucketization for all different kinds of data like audio, video and images. Then enhance the security model for the encrypted data using IND-OCPA-P model. Previous constructions proposed for efficient range queries were not secure in this model. Finally, the efficiency of the proposed scheme is discussed in terms of the number of false positives in a range query. In the proposed OB, p-1 points are selected on the uniform distribution in the plaintext-space and the plaintext-space is divided based on the selected points The proposed scheme does not consider the distribution of plaintexts because the adversary of a chosen-plaintext capability can easily break the EOB scheme if the underlying OB considers the distribution of the plaintexts. By analyzing the probability distribution of the width of a bucket in the proposed OB and checking the analysis result through experiments after implementation, the proposed scheme provided a reasonable range querying efficiency.***

I. INTRODUCTION

A novel bucketization and partitioning structure is proposed which then inflfenced many of the papers in literature. An algebraic framework is described for query rewriting over encrypted attributes.

The main idea is to map the plaintext values to ciphertext values by splitting the domain values of plaintexts into some partitions and giving them bucket ids. Each relation R (*A1, A2, ..., AN) is stored as an encrypted* relation: *RS (encrypted tuple, A1_S, A1_S, ... , A1_S) where the attribute encrypted tuple* is the encrypted string that corresponds to a tuple in R. Each attribute *Ai_S is the* index for the attribute *Ai. The domain of Ai is partitioned into partitions p1, p2, ..., pn such any two partitions do not overlap and the partitions taken as a whole cover* the whole domain. Different attributes may be partitioned using different partitions functions. These partition functions may be any two functions satisfying the above two conditions.

II. Related Work

The first approach on how to support query operations on encrypted data with bucketization, after the data is encrypted, the ciphertext is concatenated to a bucket number, which is assigned to a specific range that includes the data. When a user requests a query operation, the server uses the bucket numbers to execute the query operation. For example, if a client program wants to retrieve the data in the range between 100,000 and 200,000, it first calculates the numbers of buckets whose union is the smallest set that covers the queried range. The client program sends the bucket numbers to the database server. The database server searches all the encrypted data whose bucket number is one of the received numbers. The server then, sends the data back to the client. The client can obtain the correct result by filtering out the data that are not in the range after decrypting them. In this case, a larger amount of data transmitted between the client and server than in the case where the database stores unencrypted data items due to the false positives that occur in cases where a bucket has both the data the client wants to retrieve and data that it does not want. In OPE, the order of the underlying plaintexts can be compared only with the computation of sub-linear complexity from the ciphertexts without decrypting them. Owing to such efficiency, more efficient range queries can be supported with OPE compared to the case of using OB. Moreover, the result of range queries on ciphertexts encrypted by OPE does not produce false positives because the comparison ability on ciphertexts can distinguish whether a ciphertext has the plaintext in a specified range when the server has an encryption of two borders of the range being queried in the plaintext space.

III. Proposed System

This paper proposes the IND-OCPA-P model to analyze the security of the proposed EOB and the encryption schemes supporting an efficient range query over encrypted data.

1. The efficiency of the proposed scheme is discussed in terms of the number of false positives in a range query. The efficiency of a bucketization scheme depends on both the distribution of plaintexts and the width of a bucket.
2. The proposed scheme does not consider the distribution of plaintexts because the adversary of a chosen-plaintext capability can easily break the EOB scheme if the underlying OB considers the distribution of the plaintexts.
3. The proposed scheme and the query optimized bucketing (QOB) method were implemented to compare the number of false positives. An increase of the number of false positives was less than 3 percent.
4. A definition of OB and EOB that can be implemented with a symmetric encryption scheme is also reported. In addition, a construction of an OB where the EOB implementation is secure on the INDOCPA-P model is outlined.
5. Security analysis of an encryption scheme with the controlled diffusion bucketization the applicability of the proposed scheme to various applications in the place of OPE.

ALGORITHM: 1- Construction of Ordered Bucketization

» $K_{EOB}(p)$: Key generation algorithm,where p is the number of buckets.

1. $K \xleftarrow{\$} K$
2. $K_{OB} \xleftarrow{\$} K_{OB}(p)$
3. Return $K_{EOB}=(K,K_{OB})$

» $\pounds_{EOB}(K_{EOB}, m)$ $(m \in M)$: encryption algorithm.

1) $(K,K_{OB}) \leftarrow K_{EOB}$
2) $bucket\# \leftarrow T_{OB}(K_{OB},m)$

$

3) $c \leftarrow £(K,m)$

4) return C_{EOB} = bucket# || c

» $D_{EOB}(K_{EOB},C_{EOB})$: decryption algorithm

1) $(K,K_{OB}) \leftarrow K_{EOB}$

2) $n||c \leftarrow c_{EOB}$

3) $m \leftarrow D(K,c)$

4) return *m*

ALGORITHM: 2- Proposed EOB construction

K_{OB} *(p)*

010 $K^{p}_{bar} \leftarrow |M|-1$

$

020 for(i=1…p-1) do $K^{i}_{bar} \leftarrow M$

030 sort $(K^{i}_{bar} \ldots K^{p}_{bar})$ in ascending order

Let the result be $(k^{(1)}_{bar} \ldots, K^{(p)}_{bar})$

040 $K_{OB} \leftarrow (k^{(1)}_{bar} \ldots, K^{(p)}_{bar})$

050 Return K_{OB}

$T_{OB}(K_{OB},m)$

010 $(k^{(1)}_{bar} \ldots, K^{(p)}_{bar}) \leftarrow K_{OB}$

020 if(n € M) then return $\perp$

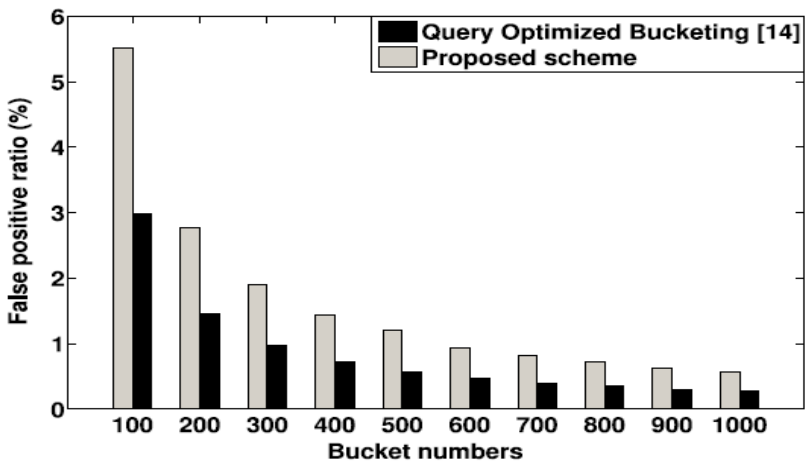
030 for(i=1…,p) do

If($m \leq K^{i}_{bar}$) then ret $\leftarrow$ i

040 Return ret

IV. PERFORMANCE EVALUATION

After the development, analyzes the efficiency of a range query over the data that is encrypted by EOB where the proposed OB is used. The main focus was to analyze the searching efficiency in terms of the false positive rate. To do this, the probability distribution of the rate of the width of a bucket to the size of the plaintext space was first analyzed to show that the width of a bucket is not skewed to be extremely large or small. This even-bucket-width property gives the proposed scheme a good querying performance on average. In the proposed OB, the p _ 1 points are randomly uniformly sampled in the plaintext space [0,|M|-1].The width of the *i*th bucket was determined by the selected points of $(i-1)^{th}$ order and i^{th} order because the width is the difference of these two points. Therefore, to analyze the width of a bucket, it is important to analyze the probability distribution of the position of the selected points.



V. CONCLUSION

A secure OB (Ordered Bucketization) was constructed with which any EOB that works on top of any IND-CPA-secure symmetric encryption scheme is secure on the IND-OCPA-P model. To analyze the security, this paper proposed a security model called IND-OCPA-P (INDistinguishability under ordered Chosen Plaintext Adversary with Polynomial querying distance) where no existing OPE and encryption with bucketization schemes have proven to be secure so far.

References

1. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf.Manage. Data, 2004
2. A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in Proc. 31st Annu. Int. Conf. dv.Cryptology, 2009
3. A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. 31st Annu. Conf. Adv. Cryptology, 2011.
4. B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proc. 30th Int. Conf. Very Large Data Bases,2004
5. L. Xiao and I. Yen, "A note for the ideal order-preserving encryption object and generalized order-preserving encryption," IACR ePrint Archive, pp. 535–552, 2012.

AUTHOR(S) PROFILE

Dr. K. Swathi obtained her under-graduation in B.E., (Computer Science & Engineering) from Bharathidasan University, Trichy in 1999. She obtained her M.E. degree in Computer and Communication Engineering from Anna University, Chennai in 2004.She obtained Ph.D degree in Faculty of Information & Communication Engineering from Anna University, Chennai in 2014. Presently, she is working as Associate Professor in Computer Science & Engineering, Cauvery College of Engineering and Technology, Trichy in 2008. She has 14 years teaching experience and also she had attended many workshops, seminars and conferences on Research issues in Image processing. She has published papers in international journals and presented papers in various Conferences. She is the life member of Indian Society for Technical Education (ISTE). Her areas of interest include Image processing, Data mining, network security and Software engineering.

S. Ramanathan, received hem M.C.A in Computer Application from Bharathidasan university, Trichy in 2010 and doing him M.E in Computer Science Engineering in Cauvery College of Engineering and Technology, Trichy. His area of interest includes Network security.

Vijayanathan. R. received his Master of philosophy Library and Information Science from Annamalai University in 1999 Also he obtained his post-graduate degree in Master of Economics in Bharathidasan University in 1996 and PG Diploma in Computer Application, PG Diploma Tourism Management and PG Diploma in co- operative management from Annamalai Unversity. He is working as a Sr. Librarian, Department of library and Information Science in Cauvery College of Engineering and technology, Trichy from 2009. He has guided many M.Phil scholars produced and member in various Universities in Tamil Nadu. He served more than 14 years as Senior Librarian in reputed Engineering College and also he had attended many workshops, seminars and conferences on Research issues in Bibliometric ananalysis.He has published so many research papers in National and International journals. His areas of interested are networking; Cloud computing, IC Technologies, Environmental study, Library Automation, Webometric study, Scientometric study, Bibliometric analysis and citation study.

