International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by

Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science, Engineering&Technologies" RASET-2015

Research Paper

A SECURE DATA ENCRYPTION USING IND-OCPA-P MODEL

N Nithya[1], S Poornimadevi[1], L Shalini[1] and M Swetha[1]

*Corresponding Author: ***N Nithya***

This is an encryption product Ordered bucketization (OB) analyzes. In OB simple space, based on the borders that they cover p from 1 top moment divided by the number of buckets. Every question is a limit to the number of cipher text by attaching a bucket that can be performed on encrypted data without the need to decrypt, OB is very useful. Unfortunately, no research cryptographic sense in existing, OB care is carried out. In this paper, OB (EOB) defines an encoding scheme and is an enemy of the legitimate authority of a new security model considers the EOB, IND-OCPA-P model, The model proposed earlier constructions efficient range queries are safe. Finally, EOB, IND-OCPA-P-India B in sample implementation is secure, the construction of an OB. In proposed 1POINTS divided on the basis of the selected points, ripples in space-uniform distribution and nature-space are selected. Each divided by a bucket in order to limit the range of numbers assigned in ascending order. A bucket of range by showing that the size distribution is skewed to a range of questions and question proposed, OB guarantees reasonably good capacity for talent in key generation should be considered in server side usage for secure purpose.

INTRODUCTION

The security for data in the Ordered Bucketization (OB) as a cryptographic object.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 .The EOB construction with the proposed OB is proven to be IND-OCPA-P-secure where d is a polynomial to the security parameter if the employed conventional symmetric encryption scheme is IND-CPA-secure. To prove this, the argument proceeds as follows. To determine if the left message is encrypted or the right message is encrypted in the IND-OCPA-P experiment, the bucket number should be different in both cases because the adversary cannot extract any meaningful information from the other part which is the output of the IND-CPA-secure encryption scheme. This paper proves that it is unlikely that the adversary will select a message pair such that, if it is given to the LR-encryption oracle, the adversary can distinguish which message of the pair is

[1] Department Of Information Technology

encrypted with a meaningful probability if d is polynomial to the security parameter. This proof means that it is highly likely that the message pairs the adversary selected are in the same bucket. By the way of encrypted format the data which can be stored in the form of ascending order. 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). In OB simple space, based on the borders that they cover p from 1 top moment divided by the number of buckets. where a range query can be supported efficiently while preserving high-level security compared to order preserving encryption. The client which sends the request in the form of query language by using QOB (Query Object Bucketization). 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 [5], [6], [14] have proven to be secure so far. To provide security by using Key Generation algorithm, the client which create a secret key for accessing data, the client which create secret key during encryption process. The server which also create secret key during decryption process. If both the key matches then the original message will be received from the server. A secure OB in multi-dimensional space will be examined by analyzing the bucketization scheme for multi-dimensional space suggested recently at [13].By the way of proposed model only the particular page is available for particular user.The user cannot able to open the multiple number of unwanted page at the same time. If the limited number of pages is used by the particular client is able to create a multi-dimensional space.

EXISTING SYSTEM

This paper introduced a new encryption scheme Encryption with Ordered Bucketization, where a range query can be supported efficiently while preserving high-level security compared to existing methods. 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 scheme. 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 .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. In future work, a secure OB in multi-dimensional space will be examined by analyzing the bucketization scheme for multi-dimensional space suggested recently.

ALGORITHMS

Symmetric Encryption

The data can be converted from plaintext to ciphertext by using encryption algorithm. By the way of encryption algorithm the data which can be arranged in the form of ascending order. To prevent the unwanted data from the user and to store only the valid information to the database. By using encryption algorithm data can be arranged in the higher range order.

Key Generation Algorithm

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/ decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data. The key generation algorithm can be implemented by creating secret key. The client which creates a secret key during encryption process, the created secret key can be used to access the information which is stored in the database. The data to be secured by using key generation algorithm and to prevent data from the unauthorized person. The created secret key matches to the database server if it matches both the keys then the data can be accessed.

Decryption Algorithm

Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext. A decryption algorithm takes an encrypted message and restores it to its original form using one or more keys. A decryption key consists of a random string of numbers, from 40 through 2,000 bits in length.

Proposed System

A secure OB in multi-dimensional space will be examined by analyzing the bucketization scheme for multi-dimensional space suggested recently .By the way of proposed model only the particular page is available for particular user. The user cannot able to open the multiple numbers of unwanted pages at the same time. If the limited number of pages is used by the particular client is able to create a multi-dimensional space. The 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. Because this model allows an adversary to query an encryption of a chosen message, it is stronger than the security model on which the construction reported in reference was proven secure.

MODULES

Encrypted Data

A 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 cipher text, where bucket refers to the bucket number of messages that are encrypted; and the bucket number is the result of OB, and the cipher text part is the result of the conventional symmetric encryption. An OB construction is proposed, where the EOB construction is secure on the IND-OCPA-P model if d is polynomial to security parameter. In the proposed OB construction, p1 points are selected uniformly in the plaintext space. When a plaintext message is given as an input of OB to retrieve the bucket number of the message, the tagging algorithm of OB returns i as the bucket number if the input message is in the range.

IND-OCPA-P Security Model

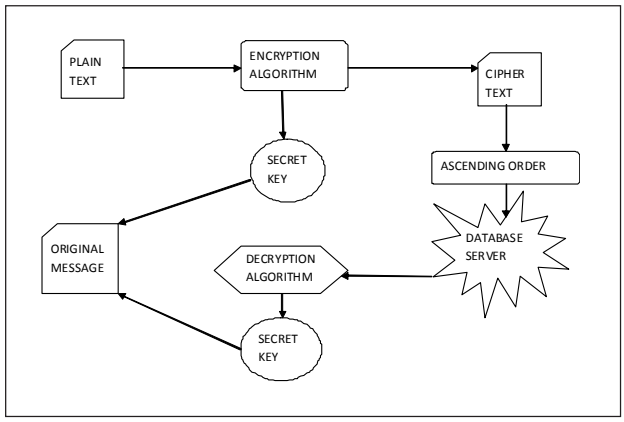
This paper proposes the IND-OCPA-P model to analyze the security of the proposed EOB and the encryption schemes supporting an efficient range query over encrypted data. Because this model allows an adversary to query an encryption of a chosen message, it is stronger than the security model on which the construction reported in reference was proven secure.

Security Analysis

Security on IND-OCPA model. Unless there is only a single bucket in M, the adversary trivially wins in this model bucket number for the plaintext 0 and the bucket number for the plaintext jMj _ 1 are different from each other. Therefore, an adversary can be constructed easily requiring only a single query to obtain a non-negligible advantage . The only need is to query ð0; jMj _ 1Þ. Then, if the index in front of the result of the query is p, the adversary returns 1 else it returns 0. In this case, the probability that the adversary wins is 1 _ 1 jMjp_1 because in the Expind-ocpa-0 SE AÞ, the probability that the encryption of 0 has p as an index is 1 jMjp_1.10.

SYSTEM FLOW DIAGRAM

In this system flow diagram represents the, how to perform encryption, key generation and decryption algorithm. The plaintext is converted into cipher text by using encryption algorithm. The way of encryption algorithm the data which can be arranged in the form of ascending order. To prevent the unwanted data from the user and to store only the valid information to the database. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/ decrypted. The key generation algorithm can be implemented by creating secret key. The client which creates a secret key during encryption process, the created secret key can be used to access the information which is stored in the database. where bucket refers to the bucket number of messages that are encrypted; and the bucket number is the result of OB, and the cipher text part is the result of the conventional symmetric encryption.



CONCLUSION

This paper introduced a secure multidimensional space, where a range query can be supported efficiently while preserving high level security compared to existing methods, By the way of proposed model only the particular page is available for particular user. The user cannot able to open the multiple number of unwanted page at the same time. If the limited number of pages is used by the particular client is able to create a multi-dimensional space. In future work ,a attach and detach analysis services databases administrator want to a offline period.

REFERENCES

1. Agrawal R, Kiernan J, Srikant R, and Xu Y (2013), “Order preserving encryption for numeric data,” in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2013, pp. 563–574.
2. Yao B, Li F, and Xiao X (2014), “Secure

Nearest Neighbour Revisited," proc.IEEE 27th Int'l Conf,Data Eng.(ICDE).2014 (http://www.qhull.Org/,2014).

3. Boldyreva A, Chenette N, Lee Y, and O'Neill A (2009), "Order-preserving symmetric encryption," in Proc. 31st Annu. Int. Conf. Adv. Cryptology, Vol. 5479, pp. 224–241.
4. Boldyreva A, Chenette N, and O'Neill A (2014), "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. 31st Annu. Conf. Adv. Cryptology, Vol. 6841, pp. 578–595.
5. Boneh D and Waters B (2014), "Conjunctive, subset, and range querieson encrypted data," in Proc. 4th Conf. Theory Cryptography, pp. 535–554.
6. Hore B, Mehrotra S, Canim M and Kantarcioglu M (2012), "Secure multidimensional range queries over outsourced data", *The Very Large Data Bases J.*, Vol. 21, pp. 333 -358.
7. Kolesnikov V and Shikfa A (2012), "On the limits of privacy provided by order-preserving encryption", *Bell Labs Tech. J.*, Vol. 17, No. 3, pp.135-146.
8. Malkin T, Teranishi I and Yung M (2013), "Order-preserving encryption secure beyond one-wayness", *IACR Cryptology ePrint Archive*.
9. Popa R A, Li Fand Zeldovich N (2013), "An ideal-security protocol for order-preserving encoding", *Proc. IEEE Symp. Security Privacy*, pp. 463 -477.
10. Xiao L and Yen I (2012), "A note for the ideal order-preserving encryption object and generalized order-preserving encryption", *IACR ePrint Archive*, pp. 535 -552.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com