BioGecko

Vol 12 Issue 03 2023

ISSN NO: 2230-5807

ENCRYPT SECURE DATA'S WITH ORE

Mrs. Subbulakshmi R[1], Austin SS[2], Elavarasan E[3], Logha Priya A[4], Sanmathi M[5],
Assistant Professor[1], UG Student[2,3,4,5]Computer Science and Engineering Karpagam Institute of Technology Coimbatore, India.

Abstract— *In Software any illegal action or violation is often reported to an administrator, centrally recorded using a security information and event management system, or both. When conducting a search or updating the database, content privacy prevents information from leakingon the changed points. This security concept finds the leak. Big data storage and privacy protection issues indeed exist, but they compromise data accessibility, so here is an order of proposed solutions exposing encryption that is both hybrids.*

Keywords —Content privacy, Privacy attacks, Privacy protection.

I. INTRODUCTION

The Internet's enormous volume of resources and powerful computation, cloud computing can effectively store and process data there. The demand for large data collection, analysis, andprocessing has increased with the advent of the cyberization era, leading to substantial compute overhead that is incompatible with local equipment. Users with limited resources can get significant advantages by outsourcing computing to the cloud. However, it is challenging to fully trust cloud computing due to its dynamic, random, and open character. Private user information may be disclosed, substantially compromising user privacy and endangering data security. As a result, users of the cloud prefer to encrypt their sensitive data first before outsourcing the ciphertext to the cloud.

Access control is generally provided by database systems as a way to limit access to sensitive data. When sensitive data is accessible through the proper database system interfaces, this method safeguards its privacy. Access control, while essential and significant, is frequently insufficient. A trusted technology for safeguarding sensitive data is encryption. Unfortunately, database systems have unwanted performance reduction when current encryption methods are integrated with them.

The encryption method known as OPES (Order Preserving Encryption Scheme), which enables comparison operations to be carried out directly on encrypted data, leaks a great deal of additional information by nature.
Range queries on encrypted data can be answered using ORE without encountering the same inherent restrictions as OPE.

Our objective is to develop and analyze ORE in a provably secure manner while simultaneously researching the use of order-revealing encryption in practical settings. The database and security industries have paid close attention to OPE's research. The first formal security definition of the OPE scheme was put forth by Boldyreva et al. Therefore, several researchers have created certain stateful and immutable methods, such as Popa et al, Kerschbaum et al, and others, in order to achieve IND-OCPA security. These methods are, however, impractical due to client storage and frequent, intense interactions. Even if OPE scheme surpasses IND-OCPA security, assaults continue to occur.

II. RELATED WORK

There are still significant security events that result in significant amounts of sensitive data leakingat the cloud storage layer due to management ignorance and deliberate attack. Companies and

governments can no longer store all of the data on their own due to the growing volume of data. Theyare more inclined to save their private information on distant, maybe unreliable servers.

Data availability is sacrificed in order to maintain data security, however encrypted databases have emerged as a powerful way to address the issues of huge data storage and privacy protection. It is challenging to query the data once it has been stored on the server as ciphertext without first decrypting it.Recent privacy assaults have multiplied quickly, drastically eroding.

Clarify the concept of content privacy in terms of security. While the content privacy concept prevents leaking on the updated points of the database during both search and update, this security idea detects leakages. None of the analogous works currently in existence can guarantee content privacy due to the inherent leakages connected with range queries, whereas the architecture of our structures prevents such leakages.

Real-world occurrence brought about by fraudulent loan applications On Wednesday, a resident of Mumbai committed suicide after it is claimed that online scammers shared an altered nude photo with his friends and family after he failed to pay back loans totaling Rs 6,000 obtained through an instant lending mobile app. While gathering data regarding loans, the rapid lending apps have access to the victim's mobile data.

III. EXISTING SYSTEM

Instead, we provide a security concept inspired by PRFs and similar primitives that requires an OPE scheme to appear "as-random-as-possible" while adhering to the order-preserving condition. After that, we create a productive OPE scheme and demonstrate its security according to our theorybased on the pseudo randomness of the underlying block cypher. Our design is based on a relationship we discover naturally between a random order-preserving function.

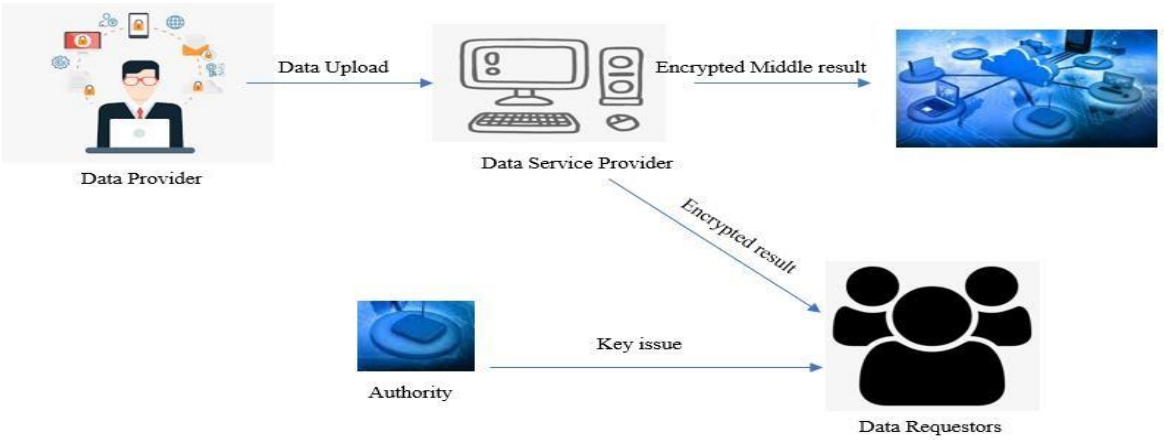

Fig 1: Order Preserving System

A cryptographic technique called order-preserving encryption (OPE) keeps the order of plaintexts. Executing range queries in encrypted databases has been a challenge for several OPE methods in recent years. OPE, however, leaks some specific information (for instance, the order of ciphertext), making it open to numerous attacks. Order-revealing encryption (ORE) was subsequently developed.

DISADVATAGE

• Range queries in encrypted databases leak specific data (for instance, the order of ciphertext), making them open to several assaults.

• Encrypted databases become exposed when specific data (such range queries) and the order of ciphertext are stolen.

IV. PROPOSED SYSTEM

Order-revealing encryption (ORE), a more adaptable idea, was presented in order to increase security and increase usability. One could consider ORE to be a generalization of OPE. Higher security is attained by ORE by tolerating a few minor leakages. The widespread consensus is that these leaks won't result in significant security losses. Additionally, ORE does not restrict the ciphertext to any certain formats. In other words, unlike the OPE system, the ciphertext in ORE is not always numerical.

In ORE, a comparability function that is publicly computable determines the order of the ciphertext. Many ORE systems have been put forth, including the fact that most ORE schemes utilize intricate cryptographic primitives (such as the property-preserving hash, or PPH) to minimize leakage.

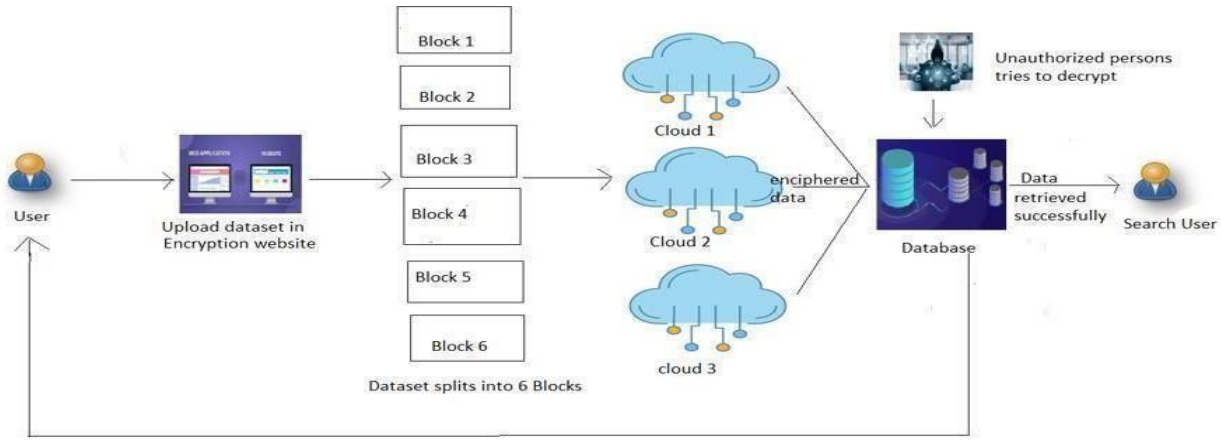

Fig 2: System Diagram

However, the Cash technique is less useful in real-world situations than those that rely solely on symmetric encryption primitives. As a result, the ORE plan still has to balance practicality with leakage. The two most well-known ORE schemes are the ones suggested. The analyses in 2019 indicated that Chenette et al.'s (CLWW) ORE scheme is the most effective one. It does, however, highlight the most important bit that differs between the two ciphertexts. Two ORE techniques were suggested by (Lewi-Wu) to further reduce leakage. The first one (Lewi-Wu-tiny) is for a tiny plaintext domain, while the second one (Lewi-Wu-Normal) is for a big plaintext.

In this study, we provide a new ORE model based on Lewi Wu-Normal and CLWW that can decrease leakage while maintaining practicality. We suggest a new ORE strategy that shortens the ciphertext based on the new ORE model.

V. MODULE DESCRIPTION

ENCRYPTION MODULE

This module comprises of a registration form or page where the user must enter the necessary login information before being sent to a page for uploading files. Here, the administrator encrypts the private data that has been submitted for security reasons in our online application. As soon as a user uploads a file, they are sent to a storage procedure where the data is split into six blocks and encrypted before being stored in three clouds.

As soon as a user uploads a file to our website, it is sent to a storage procedure where the data is divided into 6 blocks and encrypted before being stored in 3 clouds. The AES Algorithm is employedfor this Encode ORE approach.

STORAGE MODULE

Storage module that is merely a database, The data uploaded for the secured process has been movedto storage on a cloud server after the encryption procedure by dividing the data into 6 blocks of code.To store the six encrypted blocks of code, three separate clouds have been built. A symmetric key supplied by the administrator or user is required to access each cloud.

DECRYPTION MODULE

The symmetric key obtained when storing the data into the cloud from the file downloading page, the encrypted data in this module can be recovered. The created key will be sent as an OTP-like message that will allow users to be found using their login information.

The user can download data using symmetric keys, but they also enable the user to see or edit data inside the module without actually downloading it. The generated key can be used to look up the user's login details and will be provided to the user as an OTP message. Aside from allowing the user to download data, symmetric keys also allow the user to view or update data within the module itself.

ALERTING MODULE

This is the final module that alerts the user if unauthorized individuals attempt to steal the data by sending notifications. This module is crucial to our system since, despite the fact that we utilize robust encryption, it has made users happy because their personal data is secure. This is the last module to deliver notifications to the user informing them when an unauthorized individual tries to steal their data.

VI. SYSTEM IMPLEMENTATION

Any illegal activity or violation is typically recorded centrally using a security information and event management system, notified to an administrator, or both. Distribution of storage via order-revealing encryption (ORE) and hybrid ORE, which describe a security concept termed content privacy, are used to realize encrypted and prevent data breaches at the storage layer. In addition, we introduce a security concept known as content privacy. Content privacy prevents leakage on the updated pointsof the database during both search and update.

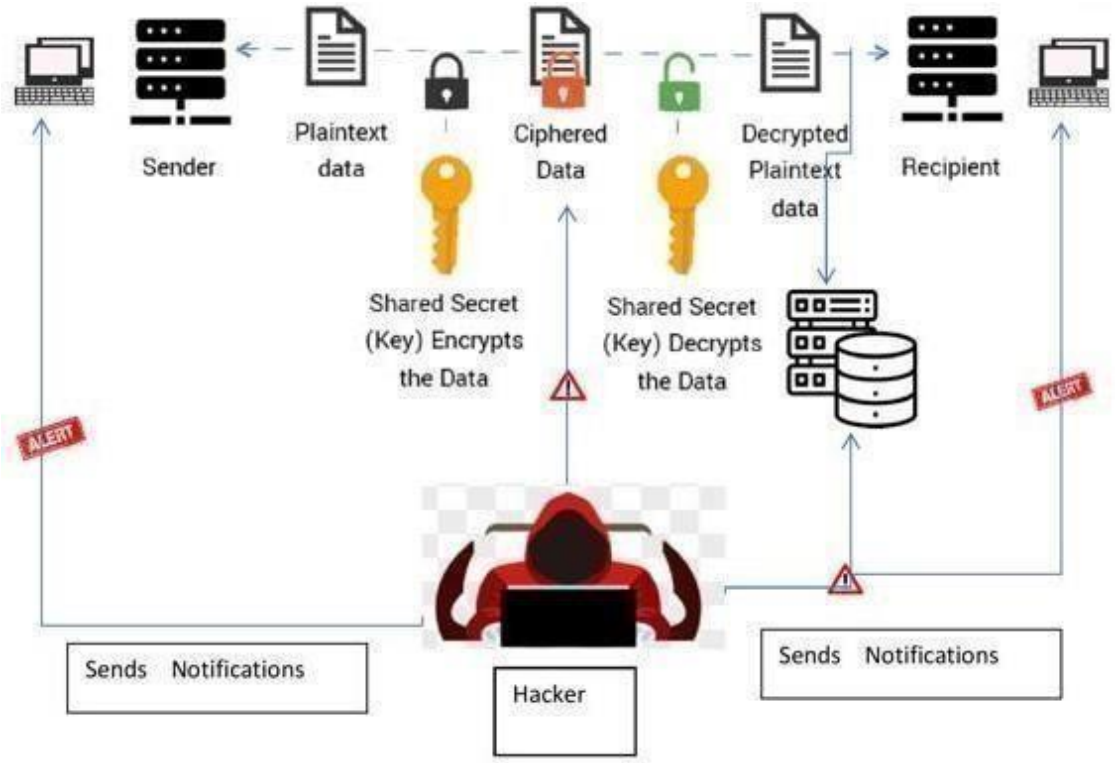

Fig 3: Process Diagram

VII. SYSTEM SPECIFICATION HARDWARE SPECIFICATION

- Processors: Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1socket, 2 cores, 2 threads per core),

- 8 GB of DRAM.
- Disk space: 2TB

SOFTWARE SPECIFICATION

- Server Side: JAVA any version(64-bit) or (32-bit)
- Client Side: HTML, CSS, JS
- IDE : NetBeans 16.
- Back end : MySQL
- Server : Apache tomcat
- OS : Windows 10

VIII. PERFORMANCE EVALUATION

Data's	OPE Order-preserving encryption	ORE Order-revealing encryption
Data Security	25%	30%
Data Leakage	10%	5%

IX. CONCLUSION

The encrypted plaintext is divided into two parts using the segmentation coding technique: the range component and the value part. We build the hybrid ORE model using the segmentation codingmethod. Then, we create the Encode ORE scheme to cut the ciphertext's length even more. We examine how much space Hybrid ORE and Encode ORE use and how much space they leak. We also conduct tests to evaluate how well Encode ORE performs.

We now have a web application system that scans network traffic for unusual activity and sends out alerts when it is found. As this application program offers.

X. FUTURE SCOPE

We intend to incorporate more intricate regulations in the future to capture privacy requirements that are independent of the dataset. Additionally, we insist on using this technique to identify fraudulent apps that obtain all of the user's rights and threaten them with their private information.

XI. ACKNOWLEDGMENT

The gratification that accompanies the successful completion of any program would be not fulfilled without mentioning of people whose unremitting cooperation made it possible, whose constant guidance and encouragement crowned all efforts with success. We are grateful and remain immensely obliged to our project guide Mrs. Subbulakshmi R, AP/CSE, KIT for the guidance, inspiration, constructive suggestions, providing us with the idea of this topic and for her invaluable support in garnering resources either by way of information or knowledge and supervision which made this project happen. We would like to say that it has certainly been a gladdening experiencefor working out this project topic.

XII. REFERENCES

[1] W. Ding, R. Hu, Z. Yan, X. Qian, R. H. Deng, L. T. Yang and M. Dong. PPC Flexible Access Control. In IEEE Trans. Network and Service Management, pages17(2): 918-930, 2020.
[2] A. Boldyreva, N. Chenette, and A. O'Neill. Orderpreserving encryption revisited: Improved security analysis and alternative solutions. In CRYPTO, pages 578-595, 2011.
[3] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill. Orderpreserving symmetric encryption.
[4] R. A. Popa, F. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proceedings of the International Conference on Security and Privacy.
[5] D. Cash, F. Liu, A. ONeill et al., "Parameter-hiding order revealing encryption," in Proceedings of the International Conference on Theory and Application of Cryptology and Information Security (Asia CRYPT), pp. 181–210, Brisbane, Australia, December 2018.
[6] Y. Li, H. Wang, and Y. Zhao, "Delegatable order-revealing encryption," in Proceedings of the International Conference on Computer and Communications Security (AsiaCCS), pp. 134–147, Auckland,

New Zealand, July 2019.
[7] H. Kadhem, T. Amagasa, and H. Kitagawa, "A secure and efficient order preserving encryption scheme for relational databases," in Proceedings of the International Conference on Knowledge Management and Information Sharing (KMIS), pp. 25–35, Valencia, Spain, October 2010.
[8] D. Liu and S. Wang, "Programmable order-preserving secure index for encrypted database query," in Proceedings of the International Conference on Cloud Computing (CLOUD), pp. 502–509, Honolulu, HI,USA, June 2012.
[9] L. Xiao, I. Yen, and D. T. Huynh, "Extending order preserving encryption for multi-user systems," IACR Cryptology, Article ID 192, 2012.
[10] J. Eom, D. H. Lee, and K. Lee, "Multi-client order-revealing encryption," IEEE Access, vol. 6, pp. 45458–45472, 2018.

AUTHORS PROFILE

Mrs. R.Subbulakshmi.,M.E., Assistant Professor, Department of Computer Science and Engineering, Karpagam Institute of Technology. She completed her Master of Engineering in Computer Science and bachelor degree in Computer Science. Her current of area of research is Encryption. She has 5 years' experience in this field and attended various workshops and conferences relatedto Machine Learning.

Mr. SS.Austin, currently pursuing B.E Degree in Computer Science and Engineering at Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India. He has attended conferences, workshops and seminars. His areas of interests are Operating System and Data Structure. He has received certain certification in the field Web Development in IBM.

Mr. E.Elavarasan, currently pursuing B.E Degree in Computer Science and Engineering, Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India. His areas of interests are Web Development and Cybersecurity. He had attended workshops and seminars based on these. He had done some certifications in the field of Cybersecurity and Web Development. He had participated in Java Programming contests.

Ms. A.Logha Priya, currently pursuing B.E Degree in Computer Scienceand Engineering, Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India. She has received certifications in the field of Web Development. Her area of interests includes web technologies and Java Programming. She also has participated in National Level Technical Symposium.

Ms. M.Sanmathi, currently pursuing B.E Degree in Computer Scienceand Engineering, Karpagam Institute of Technology, Coimbatore, Tamil Nadu, India. She has received certifications in the field of Java Programming and Python. Her area of interests includes Database Management System and Data Structure. She also has participated in Milestone PRP in Wibro and Learnathon by ICT.