International Journal for Modern Trends in Science and Technology, 8(09): 178-180, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809037
Available online at: http://www.ijmtst.com/vol8issue09.html

Personalized Forward Search with Symmetric Search Encryption

B Naga Sailaja [1] | P Srinivasa Reddy [2]

[1]PG Scholar, Department of Computer Science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
B Naga Sailaja and P Srinivasa Reddy. Personalized Forward Search with Symmetric Search Encryption. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 178-180. https://doi.org/10.46501/IJMTST0809037

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

Searchable symmetric encryption (SSE) has been broadly implemented in the encrypted database for queries in exercise. even though SSE is strong and characteristic-rich, it is constantly plagued by using statistics leaks. a few recent assaults point out that ahead privateness which disallows leakage from replace operations, now will become a fundamental requirement for any newly designed SSE schemes. but, the subsequent search operations can nevertheless leak a widespread quantity of statistics. To further strengthen protection, we extend the definition of forward privacy and advise the belief of "ahead seek privacy". Intuitively, it calls for search operations over newly delivered files do now not leak any statistics approximately beyond queries. the enhanced safety perception poses new challenges to the layout of SSE. We cope with the challenges through developing the hidden pointer technique (HPT) and suggest a new SSE scheme referred to as Khons, which satisfies our security perception (with the unique forward privacy belief) and is also efficient. We carried out Khons and our experiment effects on huge dataset (wikipedia) show that it's miles more green than current SSE schemes with ahead privacy.

KEYWORDS: Encrypted web application, data privacy, format-preserving encryption, shadow DOM, cloud storage

1. INTRODUCTION

Outsourcing of data storage is becoming more and more common, thanks to the rise of cloud computing. While the consumers benefit from features like low cost and widespread access, data privacy becomes a significant worry. Users typically encrypt data before uploading it to an unreliable storage service to preserve data privacy. However, encryption renders data unintelligible, preventing conventional retrieval techniques like the keyword search from being used on cypher texts directly. Searchable symmetric encryption (SSE) was developed in 2000 to address this issue [11]. By supplying a token that cryptographically encodes the desired keyword, a client can save encrypted documents on an untrusted server and later retrieve all documents containing that keyword.SSE is now often utilised in encrypted databases [1–7] and emails [8]. Take the Crypt DB [4] as an example. It employs SSE to handle SQL equality queries (=,!=, IN, NOT IN, etc.) when the values in the column are not unique in addition to providing SQL LIKE operator by utilising an SSE scheme [11]. SSE has recently been suggested to allow rich queries, such as conjunctive _query [9], range query [12], and others [5].

To allow equality query across the encrypted NoSQL databases, ARX has also implemented SSE.

2. LITERATURE SURVEY

Several different schemes have been proposed with the general goal of enabling data to be outsourced, while providing some kind of search functionality to data clients. Here, we review those most relevant to our work Oblivious RAM. Oblivious RAM (ORAM) [15] supports access to an outsourced memory while hiding the access pattern. Different variants of ORAM have been used to minimize the SSE leakages [5, 14, 16, 29]. However, it does not prevent the access pattern leakage [24] since the server needs to learn the list of files to retrieve. To avoid search pattern leakage and provide forward privacy, as in Stefanov et al.'s design [29], the server cost scales sublinearly with the total number of (keyword, file ID) mappings (N), not just size of the result (d).

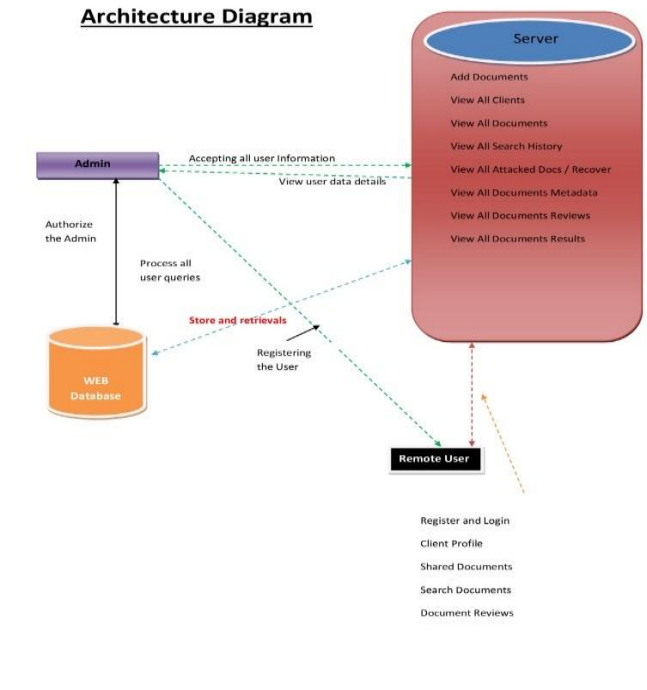
Static schemes. When the outsourced data is intended only for archiving, no update mechanisms are needed. The constructions proposed by Chang and Mitzenmacher [10] support static outsourcing with O(n) search time. Curtmola et al. [12] defined CKA2-security for SSE, and proposed adaptively and non-adaptively secure schemes under this definition, with optimal search time, linear in the size of the response. Chase and Kamara [11] gave constructions operating on matrices, labeled data, and graphs. Cash et al. [9] support Boolean search

Dynamic schemes. A dynamic SSE scheme provides operations to update encrypted data. Update operations leak more information about the outsourced data. For instance, adding a new file containing a keyword w after searching for w, reveals to the server that this new file also contains w [10, 29]. Table 2 summarizes dynamic SSE schemes.

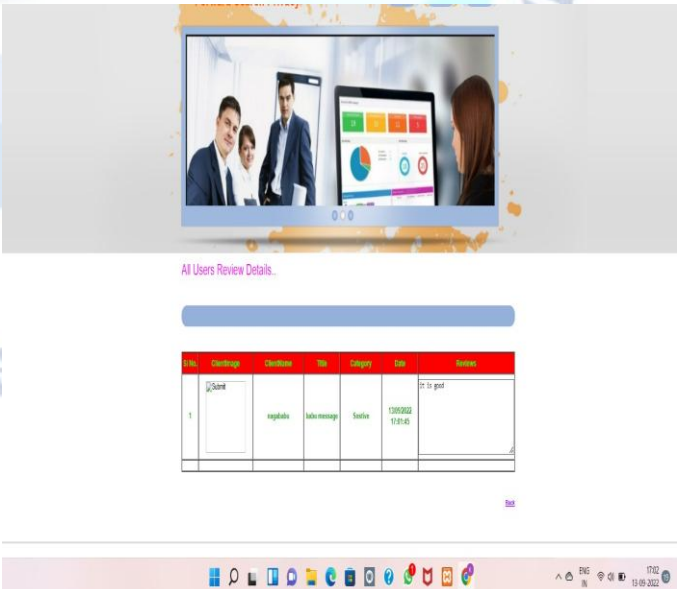
3.PROBLEM STATEMENT

In 2016, Zhang et al.proposed the file-injection attack. This attack assumes that the adversary can inject files, i.e. to craft a set of documents and trick the client into encrypting them. By injecting the carefully selected files, the adversary can recover keywords, which should be kept private, from search tokens submitted by the client. The attack is very effective and requires only a small number of files to be injected. The problem highlighted by this attack is that the security notion widely used in the past is too weak. More specifically, it allows the adversary to gain knowledge about keywords queried in the past by relating past submitted token to newly updated files. The attack calls for a more stringent treatment of information leakage in SSE and makes forward privacy the baseline for newly developed SSE schemes.

4. ARCHITECTURE



5.RESULTS



6.CONCLUSION

In this study, we introduced the idea of "forward search privacy," which makes sure that a search over recently added documents doesn't reveal information about previous queries. We created the new forward private approach and concealed pointer technique to meet this security objective (HPT). Finally, we developed the Khons strategy to provide backward and forward search privacy. The results of the experiments demonstrate how effective and useful Khons is. Although Khons can accept partial queries, our solutions' application possibilities could be somewhat constrained. Additionally, our method can only produce mediocre forward search security. We will focus on how to establish good forward search security in our next work.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] CipherCloud, "Cloud data encryption", URL: http://www.ciphercloud.com/technologies/encryption/.

[2] M. Bellare, A. Boldyreva, A. ONeill. Deterministic and Efficiently Searchable Encryption. In CRYPTO, pages 535-552, 2007.

[3] S. Tu, M. F. Kaashoek, S. Madden and N. Zeldovich. Processing analytical queries over encrypted data. In VLDB, pages 6(5): 289-300, 2013.

[4] R. A. Popa, C. Redfield, N. Zeldovich and H. Balakrishnan. CryptDB: protecting confidentiality with encrypted query processing. In SOSP, pages 85-100, 2011.

[5] S. Faber, S. Jarecki, H. Krawczyk, N. Quan, M. Rosu, and M. Steiner. Rich queries on encrypted data: Beyond exact matches. In ESORICS, pages 123-145, 2015.

[6] D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M. C. Rosu and M. Steiner. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. In NDSS, pages 23-26, 2014.

[7] I. Demertzis, D. Papadopoulos, C. Papamanthou. Searchable Encryption with Optimal Locality: Achieving Sublogarithmic Read Efficiency. In CRYPTO, pages 371- 406, 2018.

[8] W. He, D. Akhawe, S. Jain, E. Shi and D. Song. Shadowcrypt: Encrypted web applications for everyone. In CCS, pages 1028-1039, 2014.

[9] R. Li and A. X. Liu. Adaptively secure conjunctive query processing over encrypted data for cloud computing. In ICDE, pages 697-708, 2017.

[10] S. Garg, P. Mohassel and C. Papamanthou. TWORAM: Efficient oblivious RAM in two rounds with applications\ to searchable encryption. In CRYPTO pages 563-592, 2016.

[11] D. X. Song, D. Wagner and A. Perrig. Practical techniques for searches on encrypted data. In S&P, IEEE, pages 44-55, 2000.

[12] I. Demertzis, S. Papadopoulos, O. Papapetrou, A. Deligiannakis and M. Garofalakis. Practical private range search revisited. In SIGMOD, ACM, pages 185-198, 2016.

[13] E. Stefanov, C. Papamanthou and E. Shi. Practical Dynamic Searchable Encryption with Small Leakage. In NDSS, pages 72-75, 2014.

[14] M. S. Islam, M. Kuzu and M. Kantarcioglu. Access Pattern disclosure on Searchable Encryption: Ramification,\ Attack and Mitigation. In NDSS, 2012.

[15] D. Cash, P. Grubbs, J. Perry and T. Ristenpart. Leakageabuse attacks against searchable encryption. In CCS, ACM, pages 668-679, 2015.

[16] Y. Zhang, J. Katz and C. Papamanthou. All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption. In USENIX Security

Authors Biography

B.Naga Sailaja currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, Web Technologies, Operating Systems, Data Science and Artificial Intelligence.

P.Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University. His research interests include Operational, Research ,Probability and Statistics , Design and Analysis of algorithm , Big Data Analytics