Searchable Encryption for Geo-Referenced Data

Jordi Ribes González *

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
jordi.ribes@urv.cat

Abstract. Searchable encryption schemes allow users to outsource a dataset in an encrypted form while preserving the ability to remotely and privately query over it. In this work we propose different techniques for searchable encryption that achieve range queries on two-dimensional geo-referenced data. The proposed techniques improve previous works from an efficiency and from a security point of view.

1 Introduction

The cloud computing paradigm offers very convenient data storage and computation services at a low cost, thus providing an attractive alternative to physical storage and self-managed servers. Nevertheless, even though cloud computing leads to many economical and functional benefits, the action of leaving data at the hands of an external cloud service provider poses many security and privacy concerns.

One way to address the security concerns that arise from the process of outsourcing data to the cloud is providing users with user-centered cryptographic techniques. However, it is not convenient to outsource encrypted data by using traditional encryption techniques, since any operation over the dataset must be carried out locally. To overcome this obstacle, alternative cryptographic schemes must be applied.

In recent years there have been important advances in cryptographic techniques that allow to take advantage of the cloud benefits while securing the data. For example, two of these techniques are homomorphic encryption and order-preserving encryption, allowing for remote computations and ordering on encrypted data respectively.

Searchable encryption [11,3,1,4,7] deals with the problem of remotely querying over encrypted data. By using searchable encryption schemes, it is possible to outsource a dataset in an encrypted form, while preserving the searching functionality by letting users be able to send encrypted queries to

* PhD advisor: Oriol Farràs Ventura

the cloud. In this way, users can remotely and securely query over encrypted data and retrieve the segment of the outsourced dataset satisfying the query conditions.

2 Searchable Encryption for Geo-Referenced Data

Our aim is to provide searchable encryption schemes that enable a client to delegate an encrypted version of a geo-referenced dataset to a semi-trusted, honest-but-curious server, in such a way that searching capabilities over the encrypted data are preserved.

In our setting, the client first delegates an encrypted version of its dataset to a server. Such a dataset consists of a collection of documents, each of which is attached to a particular geographical point. Afterwards, the same client may want to retrieve a subset of the outsourced dataset. By generating an encrypted query, it is able to recover the outsourced documents lying inside a chosen rectangular location.

Based mainly in the works by Shi et al. [10] and by Faber et al. [6], we develop four techniques for searchable encryption achieving two-dimensional range queries over encrypted data. These techniques show different efficiency and security trade-offs. The provided solutions are also general, in the sense that they make use of an arbitrary underlying keyword searchable encryption scheme. By changing this underlying scheme, different efficiency and security measures can be achieved.

We analyze the trade-off between performance, security and communication overhead of the presented options by considering the scheme by Cash et al [4] as the underlying searchable encryption scheme. Our solutions take advantage of the Boolean search and inverted index properties of [4].

As a novel approach with respect to previous works, we build on alternative combinatorial structures to lower the leakage of the schemes, thus improving security at the cost of increasing the query size and the search time. We also present a technique based on over-covers [6] that notably reduces the communication cost and the leakage of the queries at the expense of increasing the false-positive rate.

The proposed results have been presented at the 15th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2016).

Acknowledgement. This work is partly supported by the European Commission under the H2020 project "CLARUS", ref. H2020-ICT-2014-1-644024.

References

[1] D. Boneh, B .Waters. *Conjunctive, subset, and range queries on encrypted data.* In Proceedings of the 4th conference on Theory of cryptography (TCC'07), Salil

P. Vadhan (Ed.). Springer-Verlag, Berlin, Heidelberg, 535–554, 2007.

[2] C. Bösch, P. Hartel, W. Jonker, A. Peter. *A Survey of Provably Secure Searchable Encryption*. ACM Computing Surveys, 47 (2), 18:1–18:51, 2014.

[3] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. *Searchable symmetric encryption: improved definitions and efficient constructions*. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 79–88, 2006.

[4] D. Cash, S. Jarecki, C.S. Jutla, H. Krawczyk, M.-C. Rosu, M. Steiner. *Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries*. CRYPTO, 353–373, 2013.

[5] *CLARUS: A framework for user centered privacy and security in the cloud*. Horizon 2020 project H2020-ICT-2014-1-644024. `http://www.clarussecure.eu/`.

[6] S. Faber, S. Jarecki, H. Krawczyk, Q. Nguyen, M.-C. Rosu, M. Steiner. *Rich Queries on Encrypted Data: Beyond Exact Matches*. ESORICS, 123–145, 2015.

[7] S. Kamara, C. Papamanthou, T. Roeder. *Dynamic searchable symmetric encryption*. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 965–976, 2012.

[8] J. Li, E. R. Omiecinski. *Efficiency and security trade-off in supporting range queries on encrypted databases*. In Proceedings of the 19th annual IFIP WG 11.3 working conference on Data and Applications Security. Springer-Verlag, Berlin, Heidelberg, 69–83, 2005.

[9] R. A. Popa, C. M. S. Redfield, N. Zeldovich, H. Balakrishnan. *CryptDB: Protecting confidentiality with encrypted query processing*. In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP-11). 85–100, 2011.

[10] E. Shi, J. Bethencourt, T-H. Hubert Chan, D. Song, A. Perrig. *Multi-Dimensional Range Query over Encrypted Data*. In Proceedings of the 2007 IEEE Symposium on Security and Privacy. IEEE Computer Society, Washington, DC, USA, 350–364, 2007.

[11] D. X. Song, D. Wagner, A. Perrig. *Practical Techniques for Searches on Encrypted Data*. In Proceedings of the 2000 IEEE Symposium on Security and Privacy (SP '00). IEEE Computer Society, Washington, DC, USA, 44–, 2000.