Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data

Pallavi S. Bangare¹, Prasad D. Janorkar², Vivekanand R. Desai³, Shubham K. Ingale⁴, Uday S. Ahamindrakar⁵
Assistant Professor, Department of Information Technology
UG Scholar, Department of Information Technology²,³,⁴,⁵
Sinhgad Academy of Engineering, Pune, Maharashtra, India
Savitribai Phule Pune University, Pune, India

Abstract: In medical cloud computing, a patient can send her medical data to a cloud server from afar. Because medical data is highly sensitive, only authorized doctors are allowed to access it in this case. A frequent solution is to encrypt data before outsourcing it, with the patient simply sending the corresponding encryption key to the authorized doctors. However, due to the difficulties of digging through the encrypted data, the usability of outsourced medical data is severely limited. Over medical cloud data, we propose Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes. To begin, we propose a dynamic searchable symmetric encryption scheme that uses the secure k-Nearest Neighbor (kNN) and Attribute-Based Encryption (ABE) techniques to achieve two important security features: forward privacy and backward privacy, both of which are difficult to achieve in the field of dynamic searchable symmetric encryption. Then, to address the key sharing problem that plagues the kNN-based searchable encryption strategy, we suggest an improved technique. In terms of storage, search, and update complexity, our solutions outperform prior proposals. Extensive tests show that our approaches are efficient in terms of storage overhead, index building, trapdoor generation, and query.

Keywords: Health care, Searchable encryption, dynamic updating, Attribute-based encryption

REFERENCES
[7]. Chi Chen at. Al. proposed An Efficient Privacy-Preserving Ranked Keyword Search Method IEEE 2016.
[9]. Bharath K. Samantha at. Al. k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data MAY 2015.


[26]. Kalpana S. Thakare, Archana M. Rajurkar, R. R. Manthalkar, “A Comprehensive System Based on Spatiotemporal Features Such as motion, Quantized Color and Edge Features”, International Journal of Wireless and Microwave Technologies (IJWMT) ISSN 1449 (Print), ISSN: 2076-9539 (Online), Vol.1, No.3, June. 2011, DOI: 10.5815 /ijwmt


