**CONCLUSION**

On the basis of the state of the art fully homomorphic encryption techniques, we have presented constructions YI ET AL.: PRIVATE SEARCHING ON STREAMING DATA BASED ON KEYWORD FREQUENCY 165 Performance Comparison for disjunctive, conjunctive, and complement threshold queries based on keyword frequency and then a construction for a generic threshold query based on keyword frequency. Our protocols are semantically secure as long as the underlying fully homomorphic encryption scheme is semantically secure. Our construction for disjunctive threshold query is able to search for documents containing at least one of a set of keywords as by letting the threshold ti ¼ 1 for keyword ki 2 K. Our construction for generic threshold query can search for documents M such that ðM \ K1 6¼ ;Þ ^ ðM \ K1 6¼ ;Þ as [17], [18] by letting Qð1Þ K1 and Qð2Þ K2 be two disjunctive threshold queries with the threshold

ti ¼ 1 for keyword ki 2 K and \_ðQð1Þ K1 ;Qð2Þ K2 Þ ¼ Qð1Þ K1 ^Qð2Þ K2 Þ.

Therefore, their solutions are special cases of ours.

To improve the performance of our constructions, we can compress or postprocess the ciphertext of a bit in the final stage of filter program execution as. In this case, the ciphertext of a bit can have the same size as an RSA modulus asymptotically. Theoretically, any search criteria can be constructed with fully homomorphic encryption scheme in private searching on streaming data. Even if so, different queries will need different constructions. As long as the underlying fully homomorphic encryption scheme is practical, our protocols will be practical. So far, fully homomorphic encryption schemes are impractical for many applications according to, because ciphertext size and computation time increase

sharply as one increases the security level. Recently, many esearch efforts have been devoted to construct efficient fully homomorphic encryption schemes, such as the ones by. We believe that our protocols for private threshold queries based on keyword frequency will be made practical with the performance improvement of fully homomorphic encryption techniques in the future.

Privacy is gaining increasingly higher attention, and future computing paradigms, for example, cloud computing, will only become viable if privacy of users is thoroughly protected. For example, Google Alerts is a service offered by Google that notifies its users by e-mail, or as a feed, about the latest Web and news pages of their choice. As in the case of the AOL search data leak, it is not hard to imagine queries which could be privacy sensitive. With our private searching solutions, it is possible for a user to make a filtering program according to the frequencies of some classified keywords and submit it to Google, which executes the program on all latest Web and news pages. The program can notify to the user its discovery according to the search criteria specified by the user. While the program is executed by Google, the search criteria of the user can be kept confidential to Google.