EFFICIENCY ENHANCEMENTS FOR PRACTICAL TECHNIQUES FOR SEARCHES ON ENCRYPTED DATA

Pitigala Arachchillage Pansilu Madhura Bhashana Pitigalaarachchi
(179342K)

Degree of Master of Science

Department of Computer Science and Engineering
University of Moratuwa
Sri Lanka

February 2020

EFFICIENCY ENHANCEMENTS FOR PRACTICAL TECHNIQUES FOR SEARCHES ON ENCRYPTED DATA

Pitigala Arachchillage Pansilu Madhura Bhashana Pitigalaarachchi
(179342K)

Thesis submitted in partial fulfilment of the requirements for the degree
Master of Science in Computer Science

Department of Computer Science and Engineering
University of Moratuwa
Sri Lanka

February 2020

DECLARATION

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another per-son except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works

....

Pansilu Pitigalaarachchi Date

I certify that the declaration above by the candidate is true to the best of my knowledge and he has carried out research for the Masters thesis under my supervision.

....

Dr. Chandana D. Gamage Date

ACKNOWLEDGMENTS

I would like to offer my sincere gratitude for my supervisor, Dr Chandana Gamage for his valuable inputs and support towards managing this research along with my personal and professional commitments. Without his continuous help and feedback this thesis would not have been a success. Also I would like to thank him for his guidance and directions in progressing with this research as well as the entire master's programme.

My sincere thanks goes to Dr. Shantha Fernando and the rest of the staff of the department of Computer Science and Engineering for the knowledge and support given to me in this master's programme.

I would like to express my sincere appreciation for my wife, parents and family for their continuous support for my work, studies and specially this research. Finally I like to thank all my friends and colleagues who have supported me in this endeavor.

ABSTRACT

Information security has become one of the major focus areas for any organization. More often, organizations see the need of outsourcing their data storages in meeting the operational and security objectives. This gives rise to a new problem of privacy protection of the data stored with a third party. As a solution the data is encrypted before storing with a third party data service provider. Thus when the users need to process the data, the safer option is to download the data into a secure user machine and perform the operations on the decrypted data. This creates an additional overhead of having to download a large amount of data and decrypt them even to perform a simple calculation on the data stored in the encrypted form. Therefore the possibility of secure data processing at the remote third party storage has become an interesting problem to solve. In order to preserve the privacy the data cannot be allowed to be decrypted at the third party storage. One form of the solution is to facilitate computations on the data stored in encrypted form. The users can make requests from the data service provider and if the service provider can perform operations on the encrypted data itself and provide the answer the above mentioned overhead can be avoided. This brings the focus of this research on to the studying of computing on encrypted data with specific focus on searchable encryption. As pert of the research, the current literature of computing on encrypted data is studied to identify a suitable searchable encryption scheme for practical use. Followed by the literature study, an existing symmetric searchable encryption scheme is selected for a detailed study. Here a complete implementation of the scheme is proposed and the test results are analyzed. Based on the results, a keyword extraction mechanism is proposed to improve the performance of the scheme. Finally significant performance improvements, 89.83% reduction in extra space usage due to searchable encryption and 92.11% improvement in single key word search time has been achieved. In addition to that, use cases in capital markets are studied to understand the possibilities of practical use and challenges.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES