SKRIPSI

IMPLEMENTASI SEARCHABLE ENCRYPTION DENGAN KRIPTOGRAFI KUNCI ASIMETRI

KEVIN ANTONIUS JULIANTO

NPM: 2013730014

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN

2017

UNDERGRADUATE THESIS

IMPLEMENTATION OF SEARCHABLE ENCRYPTION WITH ASYMMETRIC CRYPTOGRAPHY

KEVIN ANTONIUS JULIANTO

NPM: 2013730014

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

IMPLEMENTASI SEARCHABLE ENCRYPTION DENGAN KRIPTOGRAFI KUNCI ASIMETRI

KEVIN ANTONIUS JULIANTO

NPM: 2013730014

Bandung, 18 Mei 2017

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Husnul Hakim, M.T.

Anggota Tim Penguji

Pascal Alfadian, M.Comp.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

IMPLEMENTASI SEARCHABLE ENCRYPTION DENGAN KRIPTOGRAFI KUNCI ASIMETRI

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 18 Mei 2017

Kevin Antonius Julianto
NPM: 2013730014

ABSTRAK

Di masa sekarang ini, data biasanya disimpan pada basis data atau *server* milik pihak ketiga untuk mengurangi beban berat data di komputer lokal. Data yang hak aksesnya hanya untuk orang tertentu diberikan pengamanan khusus, seperti enkripsi. Hal tersebut dilakukan untuk menghindari kemungkinan data diakses oleh pihak yang tidak diinginkan, karena basis data atau *server* milik pihak ketiga tidak dapat dipercaya sepenuhnya. Meskipun data dan informasi tersebut telah diamankan, muncul masalah baru ketika pemilik data atau pihak yang memiliki hak akses ingin mencari suatu data tertentu. Untuk melakukan pencarian terhadap data terenkripsi dalam basis data atau *server*, pencari harus mengunduh semua data yang terenkripsi dan melakukan dekripsi satu persatu pada kumpulan data tersebut. Setelah itu, pencari baru bisa mencari dan mendapatkan data yang diinginkan.

Searchable encryption adalah sebuah metode yang memungkinkan pengguna untuk menyimpan data pada *server* dalam keadaan terenkripsi. Namun data tersebut dapat diambil secara selektif dengan memberikan informasi kepada *server* sesedikit mungkin. Dalam pencarian menggunakan *searchable encryption*, hal yang perlu dijaga keamanannya adalah data hasil pencarian dan kata kunci yang digunakan untuk mencari. Kedua hal tersebut juga tidak boleh diketahui oleh pihak *server* yang melakukan pencarian. *Searchable encryption* menggunakan sebuah struktur data tambahan berupa indeks yang memungkinkan *server* melakukan pencarian secara efisien dan tetap menjaga kerahasiaan kata kunci pencarian dan data yang dicari.

Metode *searchable encryption* dapat melakukan pencarian data terenkripsi tanpa memperlihatkan informasi yang krusial. Nilai waktu pencarian dari metode *brute force* lebih rendah daripada metode *searchable encryption* tanpa menghitung waktu dekripsi. Meskipun begitu, nilai waktu pencarian dari metode *searchable encryption* berbeda tipis dengan metode *brute force*. Nilai total waktu pencarian data menggunakan metode *searchable encryption* lebih rendah daripada metode pencarian secara *brute force*.

Berdasarkan hasil pengujian yang didapatkan dari perangkat lunak yang sudah dibangun, pencarian menggunakan metode *searchable enryption* jauh lebih efisien dibandingkan dengan metode *brute force* karena metode *searchable enryption* hanya melakukan dekripsi pada data hasil pencarian.

Kata-kata kunci: *Searchable Encryption*, *Trapdoor Function*, *Public Keys Searchable Encryption*

ABSTRACT

Nowadays, data is stored at third party database or server to reduce data load on local computer. Data with access rights for certain people are given special security like encryption. It is done to avoid possibility of data got accessed by unwanted parties, because third party cannot be trusted fully. After data and information is secured, a new problem arise when owner or parties who have access rights of the data want to search for specific data. To search for encrypted data in database or server, searcher must downloads all encrypted data and decrypting the data one by one. After that, searcher can search and get the data that he wants.

Searchable encryption is a method which allow user to save a data to server in encrypted condition. However, the data can be taken selectively by giving information to server as little as possible. When searching with searchable encryption, things that need to be secured is data from searching result and keywords that used for searching. Both of these cannot be known by server to search. Searchable encryption uses an additional data structure in form of index to allow server searching efficiently while maintaining data and keywords security.

Searchable encryption method can search encrypted data without leaking crucial information. The value of search time from brute force method is lower than searchable encryption without calculate decryption time. Still and all, the value of search time from searchable encryption method is slightly different than brute force method. The value of total search time from searchable encryption method is lower than brute force searching method.

Based on result test that obtained from software that already built, searching with searchable encryption method is far more efficient compared to brute force method because searchable encryption method only decrypting data search result.

Keywords: *Searchable Encryption*, *Trapdoor Function*, *Public Keys Searchable Encryption*

Dipersembahkan untuk orang tua, saudara, diri sendiri, pembimbing dan semua orang yang telah membantu dalam proses penyusunan skripsi ini

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas selesainya skripsi yang berjudul "Implementasi *Searchable Encryption* dengan Kriptografi Kunci Asimetri". Selama pembuatan makalah pun penulis juga mendapat banyak dukungan dan juga bantuan dari berbagai pihak, maka dari itu penulis haturkan banyak terima kasih kepada :

- Orang tua dan saudara penulis yang selalu memberikan dukungan baik secara materi, motivasi, dan doa.
- Dosen pembimbing, Bu Mariskha yang selalu memberi bimbingan dan masukan selama proses pembuatan skripsi ini sehingga dapat diselesaikan dengan baik.
- Segenap dosen dan pegawai Universitas Katolik Parahyangan Bandung Jurusan Teknik Informatika yang telah memberikan motivasi dan pendidikannya kepada penulis.
- Para sahabat dan teman dari penulis yang selalu memberi dukungan dalam penyusunan skripsi ini.

Semoga seluruh pihak yang membantu dalam penyusunan skripsi ini mendapat berkah dah rahmat dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf bila terdapat kesalahan dan kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang membutuhkan.

Bandung, Mei 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di masa sekarang ini, data biasanya disimpan pada basis data atau *server* milik pihak ketiga untuk mengurangi beban berat data di komputer lokal. Data yang hak aksesnya hanya untuk orang tertentu diberikan pengamanan khusus, seperti enkripsi. Dalam hal ini, enkripsi yang digunakan bisa berupa kriptografi kunci simetri maupun kriptografi kunci asimetri. Pada kriptografi kunci simetri, enkripsi dan dekripsi data menggunakan satu kunci yang sama. Sedangkan pada kriptografi kunci asimetri, enkripsi dan dekripsi data menggunakan dua kunci yang berbeda. Enkripsi dan dekripsi memanfaatkan sistem *character encoding*. *Character encoding* digunakan untuk mengubah karakter menjadi angka sehingga dapat dienkripsi dan didekripsi.

Enkripsi dilakukan untuk menghindari kemungkinan data diakses oleh pihak yang tidak diinginkan, karena basis data atau *server* milik pihak ketiga tidak dapat dipercaya sepenuhnya. Meskipun data dan informasi tersebut telah diamankan, muncul masalah baru ketika pemilik data atau pihak yang memiliki hak akses ingin mencari suatu data tertentu. Untuk melakukan pencarian terhadap data terenkripsi dalam basis data atau *server*, pencari harus mengunduh semua data yang terenkripsi dan melakukan dekripsi satu persatu pada kumpulan data tersebut. Setelah itu, pencari baru bisa mencari dan mendapatkan data yang diinginkan. Cara tersebut terlalu banyak memakan waktu jika data terenkripsi yang disimpan banyak. Salah satu metode untuk mengatasi permasalahan tersebut ialah dengan menggunakan metode *searchable encryption*.

Searchable encryption adalah sebuah metode yang memungkinkan pengguna untuk menyimpan data pada *server* dalam keadaan terenkripsi namun data tersebut dapat diambil secara selektif dengan memberikan informasi kepada *server* sesedikit mungkin. Dalam pencarian menggunakan *searchable encryption*, hal yang perlu dijaga keamanannya adalah data hasil pencarian dan kata kunci yang digunakan untuk mencari. Kedua hal tersebut juga tidak boleh diketahui oleh pihak *server* yang melakukan pencarian. *Searchable encryption* menggunakan sebuah struktur data tambahan berupa indeks yang memungkinkan *server* melakukan pencarian secara efisien dan tetap menjaga kerahasiaan kata kunci pencarian dan data yang dicari [1]. *Searchable encryption* memanfaatkan sebuah fungsi matematika yang disebut *trapdoor function*. *Trapdoor function* merupakan fungsi matematika yang "mudah" dihitung tetapi memerlukan sebuah nilai rahasia agar dapat dihitung balik secara efisien [2].

Berdasarkan jenis kriptografi, *searchable encryption* dibedakan menjadi dua, yaitu *searchable encryption* kunci simetri dan *searchable encryption* kunci asimetri. Pada *searchable encryption* kunci simetri, pengguna mengenkripsikan datanya sendiri agar ia dapat mengatur datanya secara keseluruhan sebelum enkripsi dan menambahkan struktur data tambahan untuk memungkinkan pengaksesan yang efisien pada data yang relevan. Setelah itu, data dan struktur data tambahan tersebut dienkripsi menggunakan sebuah kunci rahasia dan disimpan pada *server*. Pada *searchable encryption* kunci asimetri, pengguna yang mengenkripsi data dan menyimpan ke *server* bisa berbeda dengan orang yang mendekripsikan. Siapa pun yang memiliki akses ke kunci publik dapat menambahkan kata kunci pada indeks pencarian, tetapi hanya pemilik kunci privat yang dapat membuat *trapdoor function* untuk menguji hasil dari kata kunci tersebut [1].

Pada skripsi ini, akan dikembangkan sebuah perangkat lunak yang dapat mencari data yang terenkripsi dalam suatu basis data. Dengan menggunakan perangkat lunak tersebut, pengguna dapat mencari data rahasia yang tersimpan pada basis data tanpa orang lain dapat mengetahui tentang data yang dicari. Enkripsi akan dilakukan dengan algoritma kriptografi kunci asimetri agar kunci yang digunakan untuk dekripsi tidak tersebar sehingga keamanan kunci dan data lebih terjamin.

1.2 Rumusan Masalah

Berdasarkan deskripsi yang telah diuraikan, dapat dirumuskan beberapa permasalahan sebagai berikut:

1. Bagaimana cara kerja dari metode *searchable encryption* dengan kriptografi kunci asimetri?
2. Bagaimana implementasi dari *searchable encryption* dengan kriptografi kunci asimetri pada perangkat lunak?
3. Apakah *searchable encryption* dengan kriptografi kunci asimetri lebih efisien daripada metode pencarian *brute force*?

1.3 Tujuan

Berdasarkan rumusan masalah yang telah dikemukakan, tujuan yang ingin dicapai dalam penelitian ini yaitu:

1. Mempelajari cara kerja dari metode *searchable encryption* dengan kriptografi kunci asimetri.
2. Mengimplementasikan metode *searchable encryption* dengan kriptografi kunci asimetri pada perangkat lunak.
3. Menganalisa efisiensi dari metode *searchable encryption* dengan kriptografi kunci asimetri dengan membandingkan metode tersebut dengan metode pencarian *brute force*.

1.4 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. *Character encoding* yang digunakan dalam enkripsi dan dekripsi adalah *character encoding* ASCII.
2. Ukuran maksimal dari data yang digunakan adalah 1 MB.
3. Lingkungan implementasi dari hasil penelitian ini adalah pada komputer lokal.

1.5 Metodologi Penelitian

Metodologi yang akan digunakan untuk menyusun penelitian ini adalah sebagai berikut:

1. Melakukan studi literatur untuk mempelajari dasar-dasar kriptografi, *trapdoor function*, algoritma RSA dan *searchable encryption*.
2. Melakukan analisis secara manual terkait penyelesaian masalah.
3. Melakukan perancangan kelas dan basis data untuk mengimplementasikan metode *searchable encryption* dengan kriptografi kunci asimetri.

4. Mengimplementasikan hasil perancangan kelas untuk *searchable encryption* dan metode pencarian *brute force*, yang digunakan sebagai bahan perbandingan, menggunakan bahasa pemrograman Java dan basis data MySQL.
5. Melakukan pengujian terhadap perangkat lunak yang telah dibangun.
6. Menganalisa hasil pengujian terhadap perangkat lunak.
7. Membuat kesimpulan berdasarkan hasil analisa.

1.6 Sistematika Pembahasan

Sistematika pembahasan dibagi menjadi beberapa bab yang akan dijelaskan sebagai berikut:

1. Bab 1 Pendahuluan
   Bab ini membahas tentang latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.
2. Bab 2 Dasar Teori
   Bab ini membahas penjelasan tentang kriptografi secara umum, algoritma kriptografi kunci asimetri RSA, metode *searchable encryption* dan *library* MySQL Connector.
3. Bab 3 Analisis
   Bab ini membahas tentang bagaimana penerapan dari metode *searchable encryption* dengan kriptografi kunci asimetri, analisis dari setiap proses dalam bentuk flowchart, dan pemaparan diagram - diagram yang dibutuhkan.
4. Bab 4 Perancangan
   Bab ini membahas tentang diagram kelas rinci, deskripsi dan fungsi dari setiap kelas yang dibangun, diagram ERD, kebutuhan keluaran dan masukan dari perangkat lunak, dan perancangan antarmuka perangkat lunak.
5. Bab 5 Implementasi dan Pengujian Perangkat Lunak
   Bab ini membahas tentang tampilan dari perangkat lunak yang dibangun, pengujian dari perangkat lunak, dan kesimpulan dari pengujian.
6. Bab 6 Kesimpulan dan Saran
   Bab ini membahas kesimpulan dari penelitian ini dan saran untuk pengembangan lebih lanjut.