PENGAMANAN BASIS DATA *POSTGRESQL* DENGAN FITUR PENCARIAN *KEYWORD* MENGGUNAKAN SSE (*SEARCHABLE SYMMETRIC ENCRYPTION*)

Diajukan untuk Menyusun Skripsi
di Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI

Oleh:

Andri Wifaldy Hasibuan

NIM: 09021281924072

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN SKRIPSI

PENGAMANAN BASIS DATA POSTGRESQL DENGAN FITUR PENCARIAN KEYWORD MENGGUNAKAN SSE (SEARCHABLE SYMMETRIC ENCRYPTION)

Oleh :

Andri Wifaldy Hasibuan
NIM : 09021281924072

Palembang, 21 Maret 2023

Pembimbing I,	Pembimbing II,
Osvari Arsalan,S.Kom., M.T	Hadipurnawan Satria, M.Sc., Ph.D.
NIP 198806282018031001	NIP 198004182020121001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP 197812222060420003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari **Jum'at** tanggal **10 Maret 2023** telah dilaksanakan ujian komprehensif skripsi oleh jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Andri Wifaldy Hasibuan
NIM 09021281924072
Judul : Pengamanan Basis Data *PostgreSQL* Dengan Fitur Pencarian *Keyword* Menggunakan SSE (*Searchable Symmetric Encryption*)

dan dinyatakan **LULUS**

1. Penguji

   Al Farissi, S.Kom., M.Comp.Sc.
   NIP. 198512152014041001 .....

2. Pembimbing I

   Osvari Arsalan,S.Kom., M.T
   NIP. 198806282018031001 .....

3. Pembimbing II

   Hadipurnawan Satria, M.Sc., Ph.D.
   NIP. 198004182020121001 .....

4. Ketua Penguji

   Rizki Kurniati, S.Kom., M.T.
   NIP. 199107122019032016 .....

Mengetahui,
Ketua Jurusan Teknik Infomatika

Alvi Syahrini Utami, M.Kom.
NIP. 19781222206042003

HALAMAN PERNYATAAN BEBAS PLAGIAT

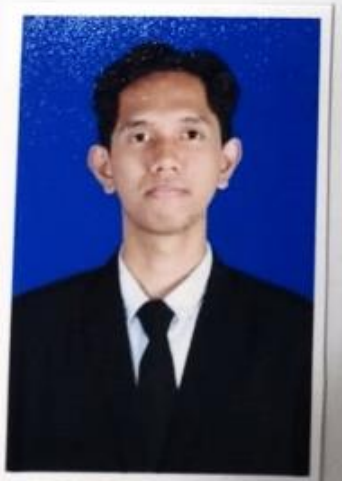
Yang bertanda tangan dibawah ini:

Nama	: Andri Wifaldy Hasibuan
NIM	: 09021281924072
Program Studi	: Teknik Informatika
Judul Skripsi	: Pengamanan Basis Data PostgreSQL Dengan Fitur Pencarian Keyword Menggunakan SSE (Searchable Symmetric Encryption)

Hasil Pengecekan Software *iThenticate/Turnitin* : 18%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil plagiat. Apabila ditemukan unsur plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Pa 2023

Andri Wifaldy Hasibuan

09021281924072

MOTTO DAN PERSEMBAHAN

!-- Being positive in all situations --!

Kupersembahkan karya tulis ini kepada:

- Orangtuaku
- Teman-teman seperjuangan
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

SECURING POSTGRESQL DATABASE WITH KEYWORD SEARCH FEATURE USING SSE (SEARCHABLE SYMMETRIC ENCRYPTION)

By:

Andri Wifaldy Hasibuan

09021281924072

ABSTRACT

PostgreSQL is a lightweight relational database that requires minimal memory usage when in operation, and it also has flexibility in choosing encryption methods as data security is crucial in a database system. However, PostgreSQL does not have the feature to search encrypted data. Therefore, this study proposes securing the PostgreSQL database with a keyword search feature using Searchable Symmetric Encryption (SSE). The study uses SSE to search for encrypted data stored in the PostgreSQL database. SSE is one method of searching for encrypted data without the need to decrypt the data being searched. In implementing SSE, a trapdoor is needed to check the data stored in the PostgreSQL database in ciphertext form. Based on the research results of the processing time comparison measurement on the PostgreSQL database query data search, an increase in processing time was found, which was 10748.12988% when searching for data using SSE, and an increase in processing time was 460.3201055% when updating encrypted data

Keywords: PostgreSQL database, cryptography, SSE, Searchable Encryption

PENGAMANAN BASIS DATA POSTGRESQL DENGAN FITUR PENCARIAN KEYWORD MENGGUNAKAN SSE (SEARCHABLE SYMMETRIC ENCRYPTION)

Oleh:

Andri Wifaldy Hasibuan

09021281924072

ABSTRAK

Basis data PostgreSQL merupakan basis data relasional yang ringan dan membutuhkan sedikit memori saat digunakan, dan juga memiliki fleksibilitas dalam memilih metode enkripsi karena keamanan data menjadi hal yang sangat penting dalam suatu sistem basis data. Namun, basis data PostgreSQL tidak memiliki fitur untuk melakukan pencarian pada data yang sudah dienkripsi. Oleh karena itu, penelitian ini mengusulkan pengamanan basis data PostgreSQL dengan fitur pencarian keyword menggunakan SSE (Searchable Symmetric Encryption). Oleh karena itu penelitian ini menggunakan SSE (Searchable Symmetric Encryption) untuk melakukan pencarian data terenkripsi yang tersimpan pada basis data PostgreSQL. SSE merupakan salah satu metode untuk melakukan pencarian data pada data yang sudah terenkripsi tanpa harus mendekripsi data yang ingin dicari. Dalam penerapan SSE, dibutuhkannya trapdoor untuk melakukan pengecekan data yang sudah disimpan dalam basis data PostgreSQL dalam bentuk ciphertext. Berdasarkan hasil penelitian dari pengukuran perbandingan processing time pada query pencarian data basis data PostgreSQL didapatkan hasil bahwa adanya kenaikan processing time sebesar 10748,12988% pada saat melakukan pencarian data dengan menggunakan SSE, dan ada kenaikan processing time sebesar 460,3201055% pada saat melakukan update data yang sudah dienkripsi.

Kata kunci: *PostgreSQL database*, kriptografi, SSE, *Searchable Encryption*.

KATA PENGANTAR

Selama penelitian dan penyusunan laporan penelitian skripsi ini, penulis tidak luput dari kendala dan hambatan. Namun demikian kendala dan hambatan tersebut dapat penulis atasi berkat bantuan, bimbingan dan dukungan dari berbagai pihak. Oleh karena itu dalam kesempatan ini, penulis ingin menyampaikan rasa terima kasih sebesar-besarnya kepada:

1. Orang tua saya yaitu Aswita Khairani Harahap dan Hardy Hasibuan serta abang dan adik yang telah memberi dukungan moril maupun materil serta doa dan restu yang tiada henti-hentinya pada penulis.
2. Bapak Osvari Arsalan,S.Kom., M.T selaku dosen pembimbing 1 dan Bapak Hadipurnawan Satria, M.Sc., Ph.D. selaku dosen pembimbing 2 yang telah membimbing, menyediakan fasilitas, memberikan motivasi terutama waktu berharganya kepada penulis dalam proses pengerjaan Tugas Akhir, hingga penulis dapat menyelesaikan Tugas Akhir dengan baik dan waktu yang cepat.
3. Ibu Dian Palupi Rini, M.Kom., Ph.D. selaku dosen pembimbing akademik, yang selalu membimbing, memberikan masukan dan motivasi kepada peneliti dalam proses perkuliahan.
4. Bapak Al Farissi, S.Kom., M.Comp.Sc. Ibu Rizki Kurniati, S.Kom., M.T. selaku penguji dan ketua penguji yang telah memberikan masukan dan dorongan dalam proses pengerjaan Tugas Akhir.
5. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Teman seperjuanganku TI Reguler B Zananda Aditya, Kurniawan Cristianto, Aditiya Rs, Naufal Kateni, Rizky Azizi, Vinito Zumizola, Giga Saputra, Indra Ghifari, Ricky Alturino, Hardian Theja, Dimas Humayun serta teman-teman lain yang tidak dapat disebutkan satu-persatu yang telah memberikan semangat dan bantuan kepada penulis.
7. Teman seperjuanganku IMMSU Sriwijaya Naufal M Daffa, Thoriq elfaridzi, Solkot Namora, Syifa Rizki, Annisa Umami, Aziza Salwa, Khairisardilla, Amalia Khairunnisa dan teman-teman lain yang tidak dapat disebutkan satu-persatu yang telah memberikan semangat dan bantuan kepada penulis.
8. Dan untuk semua pihak yang telah banyak membantu pengerjaan tugas akhir ini yang tidak dapat disebutkan satu-persatu.

Akhir kata, Penulis sangat menyadari bahwa tugas akhir ini masih jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun dari semua pihak sangat dibutuhkan dalam penyempurnaan tugas akhir ini. Semoga tugas akhir ini bermanfaat bagi semua pihak.

Palembang, 2 April 2023

Andri Wifaldy Hasibuan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada Bab I akan dijelaskan mengenai gambaran penelitian ini secara umum. Hal yang akan dibahas yaitu latar belakang masalah, rumusan masalah, tujuan dan manfaat, batasan masalah serta sistematika penulisan.

1.2 Latar Belakang

Pada era digital seperti saat ini, penggunaan basis data menjadi semakin penting karena memungkinkan organisasi untuk mengelola, menyimpan, dan mengakses informasi dengan lebih mudah dan efisien. Namun, keamanan data dalam basis data juga menjadi hal yang sangat penting untuk dipertimbangkan, mengingat informasi yang disimpan di dalamnya bisa menjadi sangat sensitif dan rahasia. PostgreSQL basis data adalah sistem manajemen basis data relational (RDBMS) yang bersifat *open-source* yang berfungsi untuk menyimpan dan mengelola data melalui perintah atau *query* SQL. Menurut (Gomes et al., 2021) PostgreSQL basis data banyak digunakan karena memiliki fleksibilitas dalam memilih metode enkripsi, memiliki performa yang baik dalam proses *query*, dan juga memiliki penyimpanan yang tinggi.

Proses enkripsi mengubah informasi asli menjadi informasi dalam bentuk sandi, sedangkan proses dekripsi mengembalikan informasi dalam bentuk sandi menjadi informasi asli. Saat ini, data dapat disimpan dalam beragam media dan

dapat dicatat sebagai *plaintext* atau dienkripsi terlebih dahulu sebagai *ciphertext*. Menyimpan data dengan cara dienkripsi terlebih dahulu memiliki kelebihan dan kekurangan. Kelebihannya adalah bahwa data yang disimpan menjadi lebih aman karena sulit untuk dibaca oleh pihak yang tidak berkepentingan. Namun, kekurangannya adalah kesulitan dalam mencari sebagian dari data tersebut. Pencarian hanya dapat dilakukan setelah dilakukan proses dekripsi terlebih dahulu. Proses dekripsi pada umumnya bersifat all-or-nothing, artinya ciphertext harus didekripsi seluruhnya menjadi plaintext atau tidak sama sekali.

Salah satu solusi untuk meningkatkan keamanan basis data PostgreSQL adalah dengan menggunakan fitur pencarian keyword yang dilengkapi dengan teknologi enkripsi simetris yang disebut SSE (Searchable Symmetric Encryption). SSE memungkinkan data di dalam basis data untuk dienkripsi dan tetap dapat dicari dengan mudah tanpa harus membuka kunci terlebih dahulu, sehingga mengurangi risiko pencurian informasi oleh pihak yang tidak berwenang.

Pada penelitian sebelumnya yang diteliti oleh (Song et al., 2000) yaitu *Practical Techniques for Searches on Encrypted Data* menggunakan *Searchable Symmetric Encryption* dalam proses pengamanan datanya. Teknik yang digunakan pada penelitian ini dapat mencari kata tanpa perlu mendekripsikan data yang ingin dicari dengan kunci simetri. Penelitian ini hanya dapat mencari satu kata saja yang ingin dicari. Dan juga pada penelitian ini, data yang sudah tersimpan pada basis data tidak dapat diperbaharui.

Penelitian lainnya yang diteliti oleh (Gomes et al., 2021) yaitu *Database Encryption for Balance Between Performance and Security* menggunakan basis

data *PostgreSQL* sebagai tempat penyimpanan data. Pada penelitian ini menggunakan algoritma AES dalam pengamanan datanya. Namun, data yang sudah dienkripsi tidak dapat kita lakukan pencariannya.

Berdasarkan uraian dan referensi penelitian sebelumnya, dengan menggunakan *searchable encryption* maka data dapat dicari tanpa harus mendekripsikan data yang ingin dicari tersebut. Hasil dari penelitian ini diharapkan dapat melakukan pencarian pada data yang sudah dienkripsi tanpa harus mendekripsi data tersebut dan juga dapat mencari data yang telah diperbaharui pada basis data *PostgreSQL*.

1.3 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penelitian ini :

1. Bagaimana mengimplementasikan *Searchable Symmetric Encryption* untuk meningkatkan keamanan data yang tersimpan pada basis data *PostgreSQL*?
2. Bagaimana hasil perbandingan *processing time* pada *query* pencarian data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi?
3. Bagaimana hasil perbandingan *processing time* pada *query update* data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengimplementasikan *Searchable Symmetric Encryption* untuk meningkatkan keamanan data yang tersimpan pada basis data *PostgreSQL*.

2. Melakukan perbandingan *processing time* pada query pencarian data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi.

3. Melakukan perbandingan *processing time* pada *query update* data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Menghasilkan skema pengamanan basis data *PostgreSQL* dengan fitur pencarian *keyword* menggunakan *Searchable Symmetric Encryption*.

2. Hasil pada penelitian ini dapat digunakan sebagai acuan untuk penelitian pada keamanan basis data *PostgreSQL* dengan fitur pencarian *keyword* selanjutnya.

1.6 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Inputan data yang ada pada aplikasi berupa teks. Tidak termasuk gambar, file dan lain sebagainya.

2. Inputan teks yang diterima hanya karakter yang terdaftar pada tabel *ASCII* dan juga *ASCII Extended*.

3. Menggunakan algoritma kriptografi *Searchable Symmetric Encryption*.

1.7 Sistematika Penulisan

Sistem penulisan tugas akhir ini sesuai dengan standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu:

BAB I. PENDAHULUAN

Bab ini memberikan informasi mengenai latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, serta sistematika penulisan.

BAB II. KAJIAN LITERATUR

Bab II kajian literatur ini menjelaskan dasar-dasar teori yang digunakan dimulai dari penjelasan mengenai kriptografi, *Searchable Encryption*, basis data *PostgreSQL*, AES (*Advanced Encryption Standard)*, RUP (*Rational Unified Process*) dan menyertakan penelitian yang relevan dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan langkah-langkah yang dilakukan dalam penelitian. Setiap tahapan dari rencana penelitian dijelaskan secara rinci sesuai dengan kerangka kerja. Bab ini juga mencakup perancangan manajemen proyek dalam pelaksanaan penelitian.

BAB IV.PENGEMBANGAN PERANGKAT LUNAK

Bab ini membahas proses dalam pengembangan perangkat lunak dalam penelitian ini. Metode yang digunakan adalah RUP (*Rational Unified Process*) yang terdiri atas proses *Inception* (Analisis kebutuhan), *Elaboration*

(Perancangan sistem, *Construction* (Implementasi perangkat lunak), dan *Transition* (Pengujian perangkat lunak).

BAB V.HASIL DAN ANALISIS PENELITIAN

Pada Bab V akan menjelaskan implementasi hasil analisis dan perancangan yang telah dilakukan sebelumnya. Hasil analisis berupa kesimpulan yang dapat ditarik dari penelitian ini.

BAB VI.KESIMPULAN DAN SARAN

Pada Bab VI terdapat kesimpulan dan saran. Isi pada Bab VI diharapkan dapat membantu meningkatkan dan mengembangkan penelitian selanjutnya.

1.8 Kesimpulan

Kesimpulan yang didapatkan pada Bab 1 ini yaitu masalah yang harus dipecahkan pada penelitian ini adalah bagaimana implementasi *Searchable Symmetric Encryption* untuk meningkatkan keamanan data yang tersimpan pada basis data *PostgreSQL*, bagaimana hasil perbandingan *processing time* pada query pencarian data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi serta bagaimana hasil perbandingan *processing time* pada *query update* data pada basis data *PostgreSQL* yang belum dienkripsi dan dengan yang sudah dienkripsi.

DAFTAR PUSTAKA

Gomes, A., Santos, C., Wanzeller, C., & Martins, P. (2021). Database encryption for balance between performance and security. *IBIMA Business Review*, *2021*. https://doi.org/10.5171/2021.614511

Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA. Proceeding SENDIU 2021, 567-568.

Krutchen, P. (2000). The Rational Unified Process An Introduction Second Edition. USA: Addison Wesley

Obe, R., & Hsu, L. (2018). PostgreSQL Up and Running: A Practical Guide to the Advanced Open Source Database. In *Livro*.

Song, D. X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 44–55. https://doi.org/10.1109/secpri.2000.848445

Thirupalu, U., Scholar, R., & Reddy, E. K. (2020). Performance Analysis of Cryptographic Algorithms in the Information Security; Performance Analysis of Cryptographic Algorithms in the Information Security. *International Journal of Engineering Research and Technology (IJERT)*, *8*(2), 64–69. www.ijert.org

Wang, Y., Wang, J., & Chen, X. (2016). Secure searchable encryption: a survey. *Journal of Communications and Information Networks*, *1*(4), 52–65. https://doi.org/10.1007/bf03391580

Yonathan, F. D., Nasution, H., & Priyanto, H. (2021). Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *7*(2), 181. https://doi.org/10.26418/jp.v7i2.47077