BAB I
PENDAHULUAN

1.1 Latar Belakang

Mudahnya akses informasi yang didapat, membawa pengaruh terhadap keamanan informasi. Seiring dengan perkembangan teknologi, semakin banyak keinginan dari pihak-pihak tertentu untuk mengambil data/informasi secara sengaja. Informasi menjadi sangat rentan untuk diketahui, diambil atau bahkan dimanipulasi dan disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab dengan masuk ke sistem melalui akses tertentu dan berusaha mendapatkan informasi yang diinginkan. Keterbatasan pengguna / petugas sistem untuk terus memantau perkembangan sistem menjadi sebuah celah bagi pihak tertentu untuk menyalahgunakan informasi yang didapat. Sebagai contoh kasus pencurian data informasi yang disengaja, seorang pegawai bank swasta yang melakukan penggelapan uang. Pelaku mengalihkan dana milik nasabah ke rekening pelaku tersebut.

Untuk mencegah pencurian data informasi seperti contoh kejadian diatas, maka suatu sistem komputer dilindindungi oleh beberapa tingkat keamanan. Diantaranya yaitu keamanan jaringan, keamanan aplikasi/program dan keamanan database. Tapi setelah melihat contoh diatas, kemungkinan lemahnya pada keamanan jaringan dan aplikasi/program, yang mudah untuk ditembus. Memungkinkan sistem komputer dapat disalahgunakan. Sehingga dengan mudahnya pihak-pihak tertentu mendapatkan dan menyalahgunkan informasi yang di dapat. Maka keamanan *Database* menjadi pertahanan terakhir ketika terjadi serangan dari pihak luar, setelah menembus keamanan jaringan dan aplikasi. (Catur, 2011)

Untuk mengawasi *user* yang memiliki wewenang memanipulasi data dibutuhkan *database management system (DBMS)* yang memiliki keamanan *database auditing*. *Database auditing* merupakan bagian dari keamanan DBMS yang bertujuan untuk memantau aktifitas yang dilakukan oleh pengguna *database*. Fitur audit ini digunakan untuk mencatat informasi, yaitu informasi aktifitas yang mencurigakan pada suatu *database* yang dilakukan

oleh *user* dengan menggunakan fasilitas *audit trail*. Fasilitas *audit trail* ini digunakan untuk mengetahui *user* mana saja dan apa saja yang dilakukan oleh objek-objek *database*. Sehingga dibutuhkan suatu sistem keamanan informasi, fokus kita untuk membahas keamanan *database*. Oleh karena itu *database auditing* merupakan salah satu masalah utama dalam keamanan informasi. Untuk membangun *auditing*, data historis atau temporal *database* diperlukan untuk melacak operasi dan tipe operasi dengan waktu. *Database auditing* dapat menjadi komponen penting dalam keamanan informasi. *Database Administrator* perlu lebih waspada dalam teknik yang digunakan untuk melindungi data, serta memantau dan memastikan bahwa perlindungan yang memadai terhadap data tersedia. (Abhisena & Githa, Agustus 2017)

Kajian terhadap *database auditing* telah dilakukan oleh beberapa penelitian sebelumnya. Beberapa diantaranya memuat teori-teori dalam mendukung proses *auditing*. Menurut (Yang, 2009) dengan penelitian berjudul *Teaching Database Security and Auditing* mengungkapkan banyak jejak audit (*audit trails*) yang dihasilkan untuk lingkungan *database*, sehingga terdapat beberapa kategori dalam auditing. Kategori audit pertama yang dibutuhkan pada kebanyakan lingkungan auditing adalah jejak audit dari log on dan log off, serta mencatat semua upaya log in yang gagal. Kategori kedua adalah auditing terhadap DCL (*Data Control Language*) pada database. DCL mencakup perubahan pada hak akses *user*, *user login*, dan atribut keamanan lainnya. Kategori ketiga adalah *auditing* terhadap DDL (*Data Definition Language*) seperti mengubah skema *database* atau tabel. Beberapa aktivitas pencurian informasi mungkin sering melibatkan perintah DDL. Kategori keempat adalah *auditing* terhadap perubahan data melalui aktivitas DML (*Data Manipulation Language*). Melalui auditing pada perintah DML, perubahan yang terjadi, baik nilai lama maupun nilai baru, dapat terekam. Kategori kelima adalah *auditing* DTL (*Data Transaction Language*) digunakan pada saat pengelolaan transaksi *database* saat sedang berjalannya operasi dan juga saat gagal untuk dijalankan. Kategori keenam adalah auditing perubahan terhadap sumber dari *stored procedure* dan *trigger*, dimana kode program untuk

kejahatan dapat dengan mudah disembunyikan. Kategori ketujuh adalah *auditing* terhadap kesalahan *database* akibat berbagai hal, seperti penyerangan database oleh pihak tertentu.

Penelitian ini menerapkan implementasi ketujuh database yaitu *auditing* untuk melakukan *audit* (*audit trails*) terhadap segala aktivitas di *database* pada transaksi dengan mempertimbangkan status operasi, waktu yang valid, dan tipe operasi menggunakan model *relasional*.

1.2 Rumusan Masalah

Rumusan masalah yang dapat diidentifikasi dalam penelitian ini diantarnya adalah sebagai berikut:

1. Bagaimana proses untuk keamanan *database*.
2. Bagaimana implementasi *auditing* (*audit trail*) untuk keamanan *database*.
3. Membadingkan proses jenis *audit trail* apa saja yang bisa di terapkan di MySQL dan PostgreSQL.

1.3 Tujuan Penelitian

Tujuan tugas akhir ini adalah:

1. Mengetahui proses keamanan *database*.
2. Mengetahui cara implementasi *audit trail* untuk keamanan *database*.
3. Mengetahui perbandingan jenis *audit trail* apa saja yang bisa diterapkan di MySQL dan PostgreSQL.

1.4 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai implementasi *auditing* untuk melakukan *audit (audit trail)* terhadap segala akivitas pada transaksi *database*.

1.5 Batasan Masalah

Untuk mencegah melebarnya masalah yang akan diteliti, maka batasan masalah dalam penilitian ini adalah:

1. Keamanan informasi yang diterapkan untuk database MySQL dan PostgreSQL dengan menerapkan tujuh kategori (*log on-log off, DCL, DDL, DML, DTL, trigger dan auditing*).
2. Jenis *auditing* yang di implementasikan pada database MySQL dan PostgreSQL audit trail.

1.6 Metodologi Penelitian

Metodologi yang digunakan untuk menyelesaikan masalah adalah:

1. *Studi Literatur*

   Studi Literatur ini dimaksudkan untuk mencari dan mempelajari konsep dari teori pendukung terhadap perancangan yaitu dari buku, jurnal, dan referensi lain yang relevan dengan mempelajari hal-hal yang berkaitan dengan perancangan.
2. *Konsultasi*

   Konsultasi ini dilakukan dengan para pembimbing, yaitu memberikan bimbingan dan arahan mengenai tugas akhir.
3. Tahap Perancangan pada tahap ini dilakukan perancangan sebuah sistem keamanan database yang dapat mendeteksi dan memblok intrusi dalam database secara otomatis.
4. Tahap Pengujian Sistem dan Analisa, pada tahap ini sistem keamanan *database* yang sudah dirancang sedemikian rupa. Sehingga dapat mendeteksi adanya penyusupan dalam database dan mengaudit secara otomatis.

1.7 Sistematika Penulisan

Dalam sistematika penulisan ini terdapat pembahasan yang tersusun dalam beberapa kelompok sehingga mempermudah dalam memahami maksud dan tujuan dalam penelitian ini.

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang permasalahan, rumusan masalah yang akan diselesaikan, batasan masalah, tujuan penelitian, metode penelitian, sistematika penulisan, dan jadwal kegiatan yang direncanakan.

BAB II LANDASAN TEORI

Bab ini membahas tentang teori-teori dasar yang berhubungan dengan permasalahan yang diambil, seperti penjelasan mengenai konsep sistem keamanan pada database. Yang diimplementasian pada DBMS MySQL dan PostgreSQL.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang penganalisaan kebutuhan dan perancangan dari sistem. Meliputi analisis sistem, analisis kebutuhan sistem, perancangan arsitektur, perhitungan manual, rancangan database, serta langkah-langkah yang akan dilakukan untuk menyelesaikan permasalahan dan mencapai tujuan yang telah ditetapkan.

BAB IV IMPLEMENTASI DAN ANALISIS

Bab ini menjelaskan tentang pengujian sistem secara umum maupun terperinci mengenai hasil penerapan sistem pada objek penelitian.

BAB V PENUTUP

Bab ini terdiri dari simpulan dan saran, yang berisi tentang simpulan hasil penelitian dan saran-saran yang dibutuhkan guna pengembangan sistem lebih lanjut


UNIVERSITAS MUHAMMADIYAH
GRESIK