
Perancangan Sistem Informasi Pembatasan Hak Akses Pengelola Data Pada Aplikasi Core Banking System Temenos T24

Ardy Iskandar¹, Saghifa Fitriana², Satya Suhada³

¹ *Universitas Nusa Mandiri*

Jl. Jatiwaringin No. 2, Cipinang Melayu, Makasar Jakarta Timur

² *Universitas Bina Sarana Informatika Kampus Kabupaten Banyumas*

Jl. HR Bunyamin 106 Pabuaran Purwokerto Utara, Banyumas

³ *Universitas Bina Sarana Informatika Kampus Sukabumi*

Jl. Cemerlang No 8 Sukakarya, Sukabumi

** Corresponding Author.E-mail: saghifa.sff@bsi.ac.id*

Abstrak

Sistem Keamanan merupakan hal yang sangat penting dalam proses mengelola data, Dibutuhkan jaminan keamanan dalam sistem informasi terutama pada aplikasi Core Banking System. Aplikasi Core Banking System yang digunakan oleh penulis adalah aplikasi Core Banking System Temenos T24. Pengelola data pada aplikasi Core Banking System Temenos T24 ini memiliki peran hak akses tercatat sebagai Super User. Super User dapat melakukan aktivitas berbagai hal (Full Control), dan aktivitas tersebut tidak dapat diketahui oleh siapa pun. Hal ini mengakibatkan semua pengguna dapat melakukan aktivitas terhadap pengguna hak akses pengelola data. Oleh karena itu, untuk menjaga keamanan aplikasi diperlukan perancangan dan pengembangan pada aplikasi Core Banking System Temenos T24. Perancangan dan pengembangan tools ini diharapkan mampu mengelompokkan hak akses pengelola data sesuai dengan peran dan wewenang, serta mampu melakukan pencatatan terhadap aktivitas penggunaan hak akses pengelola data. Pencatatan aktivitas ini menjadikan landasan informasi dari aktivitas masing – masing peran dan wewenang dari user.

Kata Kunci: Temenos T24; Core Banking System; Hak Akses

Abstract

The security system is very important in the process of managing data. Security guarantees are needed in information systems, especially in the Core Banking System application. The Core Banking System application used by the author is the Temenos T24 Core Banking System Application. The data manager in the Temenos T24 Core Banking System Application has the role of access rights registered as a Super User. Super User can perform any activity (Full Control) and this activity cannot be known by anyone. This results in all users being able to carry out activities that are not in accordance with their roles and authorities, and there is no recording of activities against users of data management access rights. Therefore, it is necessary

to design and develop the Temenos T24 Core Banking System application. The design and development of tools is expected to be able to classify data manager access rights according to roles and authorities, and to be able to record activities on users of data manager access rights. Activity recording is the basis of information from each activity - each role and authority of the user.

Keywords: *Temenos T24; Core Banking System; Access Rights*

1. Pendahuluan

Dalam kemajuan sistem informasi memiliki perkembangan data – data penting yang tersimpan dalam sistem, dibutuhkan jaminan keamanan untuk sistem informasi tersebut terutama pada aplikasi Core Banking System. Salah satu peran penting pada aplikasi Core Banking System yaitu memiliki keamanan yang sangat kuat. Hal ini agar keamanan dalam sebuah aplikasi Core Banking System dapat tersimpan dengan baik serta dapat menghindari terjadinya hal – hal yang tidak diinginkan seperti pencurian data ataupun manipulasi data – data (Lenawati, 2017).

Aplikasi Core Banking System yang dikembangkan oleh PT Anabatic Solusi Digital adalah Aplikasi Core Banking System Temenos T24. Aplikasi Core Banking System Temenos T24 ini memiliki sistem keamanan yang cukup baik. Keamanan data pada sistem ini harus terjaga dengan baik, salah satu upaya menjaga keamanan pada sistem adalah dengan melakukan pembatasan pada hak akses pengelola data (access control) dan diperlukan pencatatan setiap aktivitas yang

dilakukan oleh pengguna (Hendarsyah, 2012).

Hak akses pengelola data pada aplikasi Core Banking System Temenos T24 saat ini keseluruhan tercatat sebagai Super User. Dalam peran Super User pada sistem memiliki hak akses kendali penuh (Full Control) yaitu pengguna dapat melakukan aktivitas berbagai macam hal. Saat ini aktivitas yang dilakukan oleh pengguna tidak dapat diketahui, hal ini dapat menimbulkan ancaman terjadinya pencurian data, penggunaan atau modifikasi sistem secara illegal dan kesalahan manusia.

Berdasarkan masalah di atas, maka penulis membuat perancangan sistem bertujuan untuk memperketat sistem keamanan pada aplikasi Core Banking System Temenos T24.

2. Dasar/Tinjauan Teori

Keamanan sistem informasi tentunya berkaitan erat dengan keamanan basis datanya. Keamanan basis data adalah perlindungan basis data atas penggunaan yang tidak mempunyai hak. Tidak adanya langkah – langkah pengamanan yang tepat,

integrasi membuat data menjadi rawan. Akses dari pengguna yang diizinkan dapat dibatasi oleh operation type (Darudiato, 2006).

Keamanan sistem perlu dilakukan pengelompokan dan pembatasan pengguna hak akses (access restriction), hal ini adalah salah satu upaya menjaga keamanan sistem. Dengan melakukan pengelompokan dan pembatasan hak akses dapat menjaga kesalahan akibat dari manusia (human error), pencurian data dan penyalahgunaan kewenangan umum (Guritno, 2008). Penelitian yang dilakukan oleh Ezedine Barka, Sujith Samuel Mathew, dan Yacine Atif pada tahun 2015 dengan judul “Securing the web of things with role-based access control” menjelaskan tentang sebuah arsitektur menggunakan fitur Role – Based Access Control (RBAC) untuk menentukan kebijakan kontrol akses user dengan metode Web of Things (WoT) serta menggunakan kriptografi untuk menerapkan kebijakan semacam itu (Barka, 2015). Permasalahan yang dihadapi dari kebutuhan hak akses pengelola data saat ini masih tercatat sebagai Super User artinya Full Control hak akses untuk pengelola data pada semua user, Hal ini akan menimbulkan masalah sebagaimana user yang tidak memiliki wewenang akan hal tersebut dapat melakukan pengelola data tidak sesuai dengan peranannya (Benuf, 2021).

2.1 Konsep Dasar Berorientasi Objek

Pemrograman berorientasi Object adalah suatu cara baru dalam berpikir serta berlogika untuk menghadapi masalah – masalah yang akan dicoba atasi dengan bantuan computer. Object adalah suatu komponen yang mempunyai bentuk fisik dan biasanya dapat dilihat. Object biasanya dipakai untuk melakukan tugas tertentu dan mempunyai batasan-batasan tertentu.

Dalam penggambaran dan perancangan sistem ada cara penggambaran yang menggunakan Unified Modeling Language (UML), sebuah teknik pengembangan sistem yang menggunakan bahasa grafis sebagai alat untuk pendokumentasian dan melakukan spesifikasi sistem (Udi, 2018).

2.2. Bahasa Pemrograman

Bahasa pemrograman yang digunakan dalam Perancangan Sistem Informasi Pembatasan Hak Akses Pengelola Data Pada Aplikasi Core Banking System Temenos T24 yaitu jBC Language dan jBase Query Language. jBC Language adalah bahasa pemrograman yang digunakan dalam aplikasi Core Banking System Temenos T24. Sintaksnya seperti Basic, proses kompilasi pertama – tama mengubah kode sumber ke C yang pada gilirannya dikompilasi untuk platform target dengan menggunakan kompilator C standard.

jBase Query Language (jQL) adalah bahasa query yang digunakan dalam aplikasi Core Banking System Temenos T24. Merupakan item library yang digunakan untuk memilih dan mengurutkan baris serta dapat menampilkan kolom. Bahasa query ini mampu menghitung total kolom, rata – rata, dan persentase dengan pengubah yang sesuai diterapkan.

3. Hasil dan Pembahasan

3.1. Metode Penelitian

Model air terjun menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengkodean, pengujian, dan tahap pendukung (support). Pendekatan SDLC dengan berbagai pekerjaan di suatu tahap diselesaikan terlebih dulu sebelum pekerjaan dilanjutkan ke tahap berikutnya. Aliran SDLC sebagian besar tetap sama, berapa pun jumlah tahapannya. Siklus hidup pengembangan sistem (System Development Life Cycle) SDLC adalah metode pengembangan sistem tradisional yang digunakan oleh berbagai perusahaan untuk proyek teknologi informasi besar seperti infrastruktur teknologi informasi. SDLC adalah kerangka kerja terstruktur yang terdiri atas berbagai proses berurutan untuk mengembangkan sistem informasi. Model SDLC air terjun (waterfall) sering juga disebut model sekuensial linier

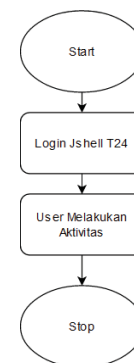
(sequential linear) atau alur hidup klasik (classic life cycle) (Rosa, 2011).

3.2. Proses Bisnis Sistem

Suatu sistem terdiri dari banyak prosedur yang saling berkaitan untuk tujuan menyelesaikan permasalahan dengan proses bisnis. Sistem yang berjalan saat ini pada aplikasi Core Banking System memiliki user dengan peran hak akses setara saat melakukan pengelolaan data. Proses pembuatan hak akses melibatkan tiga komponen utama yaitu: User, Operation System dan aplikasi Core Banking System.

3.3. Spesifikasi Dokumen Sistem Berjalan

Spesifikasi dokumen system berjalan ini tidak merincikan jenis hak akses user dan pencatatan aktifitas pada aplikasi Core Banking System



Gambar 3.3 Spesifikasi Dokumen Sistem Berjalan

3.4. Analisa dan Kebutuhan Software

Berikut merupakan spesifikasi kebutuhan (*system requirement*) dari pembatasan hak akses pengelola data:

A. Tahapan Analisis

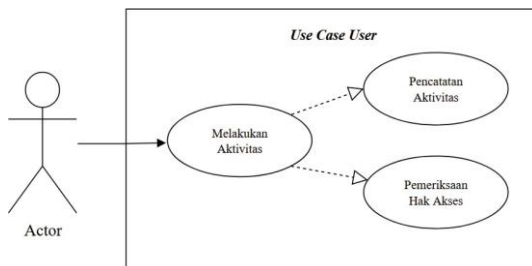
Halaman User :

User hanya dapat menjalankan query/command sesuai dengan hak akses yang diberikan mengacu pada table parameter user jshell.

Halaman Super User:

1. Super User dapat melakukan konfigurasi data pada table parameter function query.
2. Super User dapat melakukan konfigurasi data pada table parameter jshell command.
3. Super User dapat melakukan konfigurasi data pada table user jshell.
4. Super User dapat melakukan pemeriksaan pencatatan aktivitas user untuk melacak aktivitas yang telah dilakukan oleh user jshell.

B. Use Case Diagram



Gambar 3.4. B. Use Case Diagram User

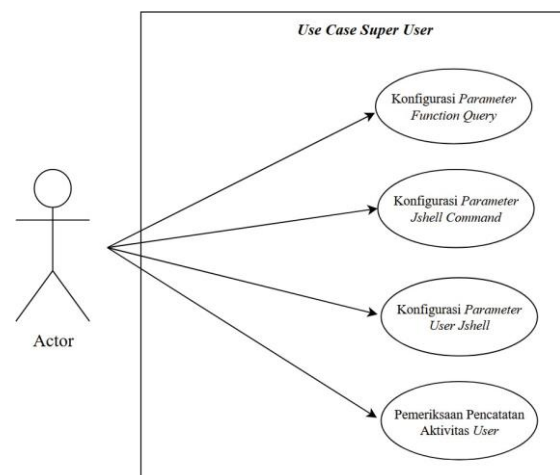
Use Case Diagram User:

Tabel Use Case Diagram User

Tipe	Dekripsi
Actor	User
Use Case	Melakukan aktivitas yang diizinkan

Tabel Aktivitas Mengelola Data

Nama	Aktivitas mengelola data
Aktor	User
Deskripsi	Use Case yang digunakan untuk melakukan aktivitas yang diizinkan
Alur Use Case	User melakukan aktivitas pengelola data kemudian aktivitas tersebut akan dilakukan validasi hak akses oleh system
Kondisi Awal	User menjalankan aktivitas pengelola data
Kondisi Akhir	System memberikan validasi terhadap hak akses tersebut



Gambar Use Case Diagram Super User

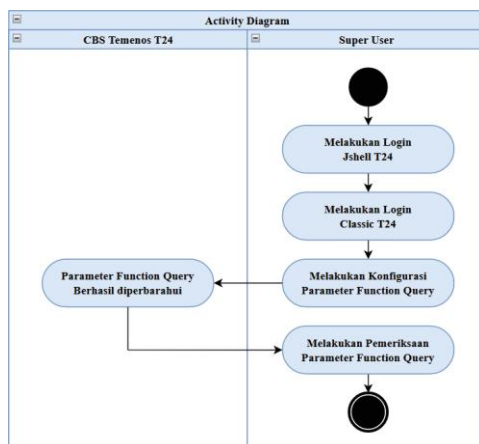
Use Case Diagram Super User:

Tabel 4.1 Use Case Diagram Super User

Tipe	Deskripsi
Actor	Super User
Use Case	Konfigurasi data table parameter function query
	Konfigurasi data table parameter jshell command
	Mengelola data table parameter user jshell
	Pemeriksaan data log table activity

C. Activity Diagram

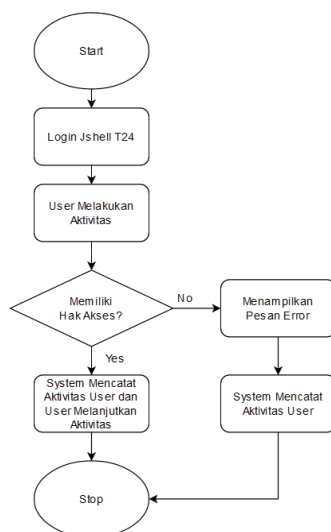
Activity Diagram adalah teknik menggambar alur kerja atau aktivitas dalam melakukan pekerjaan. Activity Diagram atau diagram aktivitas menggambarkan urutan kegiatan atau urutan aktivitas dari sebuah system.



Gambar 3.4. C Activity Diagram Konfigurasi Function Query

3.5. Rancangan Algoritma Sistem Usulan

Berikut ini rancangan algoritma sistem usulan untuk pembatasan hak akses user :



Gambar 3.5 Rancangan Algoritma Sistem Usulan

3.6. Kesimpulan

Setelah mempelajari permasalahan yang dihadapi dan juga solusi pemecahan yang ditawarkan dapat disimpulkan bahwa dengan adanya pembatasan hak akses ini semua pengguna sudah memiliki peranan sesuai dengan wewenang yang bersangkutan. Adanya pencatatan aktivitas user pengelola data, Super User dapat mengetahui hal – hal yang dilakukan oleh semua pengguna serta dapat digunakan untuk kebutuhan tracing oleh audit internal dan external.

3.7. Daftar Referensi

- [1] Lenawati, M., & Winarno, W. W. (2017). Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. Speed-Sentra Penelitian Engineering dan Edukasi, 9(1).
- [2] Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita, 1(1), 12-33.
- [3] Darudiato, S., Sam, A., & Hadi, G. P. (2006). Analisis dan Perancangan Basis Data Eksplorasi Berbasis Objek Studi Kasus Kondur Petroleum SA. In Seminar Nasional Aplikasi Teknologi Informasi (SNATI).
- [4] Guritno, S., Rahardja, U., & Setiatmi, V. (2008). Access Restriction Sebagai Bentuk Pengamanan Dengan Metode Ip Token. Creative Communication and Innovative Technology Journal, 1(3), 197-207.
- [5] Barka, E., Mathew, S. S., & Atif, Y. (2015). Securing the web of things with role-based access control. In Codes, Cryptology, and Information Security: First International Conference, C2SI

- 2015, Rabat, Morocco, May 26-28, 2015, Proceedings-In Honor of Thierry Berger 1 (pp. 14-26). Springer International Publishing.
- [6] Benuf, K. (2021). Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi. *Majalah Hukum Nasional*, 51(2), 261-279.
- [7] Udi, U. (2018). Penerapan Metode SDLC Waterfall Dalam Pembuatan Sistem Informasi Akademik Berbasis Web Studi Kasus Pondok Pesantren Al-Habib Sholeh Kabupaten Kubu Raya, Kalimantan Barat. *Jurnal Teknologi Dan Manajemen Informatika*, 4(1).
- [8] Rosa, A. S., & Salahuddin, M. (2011). Modul pembelajaran rekayasa perangkat lunak (terstruktur dan berorientasi objek). Bandung: modula, 2.