DOI: 10.47002/seminastika.v3i1.262

PEMANFAATAN CLOUD IDENTITY SEBAGAI SUMBER DATA PENGGUNA DALAM PENERAPAN OTORISASI DAN OTENTIKASI LAYANAN APLIKASI BERBASIS WEB MENGGUNAKAN LDAP DAN RADIUS (STUDI KASUS: POLITEKNIK NEGERI TANAH LAUT)

DESIGN OF SINGLE SIGN ON WEB APPLICATION USING CLOUD IDENTITY

Fathurrahmani[1*], Herpendi[2], Khairul Anwar Hafidz[3]
[123]*Teknik Informatika Politeknik Negeri Tanah Laut, Pelauihari, Kab. Tanah Laut*

[*]*E-mail: fathurrrahmani@Politeknik Negeri Tanah Laut.ac.id*

ABSTRAK

Politeknik Negeri Tanah Laut memiliki beberapa sistem berbasis web, namun semua sistem masih bersifat standalone dan belum terintegrasi, sehingga pengguna harus memiliki akun yang berbeda pada masing-masing sistem. Pengguna harus mengingat setiap akun untuk mengakses sistem dan untuk alasan keamanan biasanya pengguna mengganti passwordnya secara rutin. Proses pergantian password ini akan memerlukan waktu yang cukup lama mengingat setiap perubahan yang dilakukan berbanding lurus dengan jumlah sistem yang ada (existing). Oleh karena itu diperlukan sistem yang dapat mengintegrasikan akun pengguna dan mengelola proses autentikasi dan otorisasi. Proses ini memerlukan sebuah server tambahan yang menjadi penghubung antara sistem integrator dengan sistem layanan aplikasi. Tujuan dari penelitian ini adalah menciptakan suatu inovasi sistem yang dapat menangani seluruh otentikasi dan otorisasi setiap sistem aplikasi dan dikenal dengan sistem Single Sign On. Sehingga manfaat penelitian dari adanya sistem Single Sign On pengguna hanya dengan menggunakan satu akun pengguna dapat mengakses banyak sistem tanpa memasukkan username dan password berulang. Penerapannya data akun pengguna diambil dari Cloud Identity melalui Secure LDAP, kemudian data pengguna dikelola oleh RADIUS Server dan didistribusikan ke sistem layanan aplikasi yang ada (existing). Secara jangka pendek penelitian ini akan diterapkan di Politeknik Negeri Tanah Laut. Penelitian ini dirancang menggunakan dua aplikasi web yaitu aplikasi native php dan cms wordpress.

***Kata kunci**: sso, cloud identity, ldap, radius, autentikasi, otorisasi*

ABSTRACT

Politeknik Negeri Tanah Laut has several web-based systems, but all systems are still standalone and not yet integrated, so users must have different accounts on each system. Users must remember each account to access the system and for security reasons users usually change their passwords regularly. This password change process will take a long time considering that every change made is directly proportional to the number of existing systems. Therefore we need a system that can integrate user accounts and manage the authentication and authorization process. This process requires an additional server that acts as a liaison between the system integrator and the application service system. The purpose of this research is to create an innovative system that can handle all authentication and authorization of each application system and is known as the Single Sign On system. So that the benefits of research from the existence of a Single Sign On system, users only by using one user account can access many systems without entering repeated usernames and passwords. In practice, user account data is retrieved from Cloud Identity via Secure LDAP, then user data is managed by the RADIUS Server and distributed to existing application service systems. In the short term, this research will be applied at the v. This research was designed using two web applications, namely native php applications and wordpress cms.

***Keywords:** sso, cloud identity, ldap, radius, authentication, authorization*

PENDAHULUAN

Dunia teknologi berkembang dengan sangat cepat dan pesat. Teknologi banyak dikembangkan untuk berbagai macam keperluan bagi penggunanya. Teknologi memiliki manfaat yang sangat besar terutama dalam pengolahan data dan informasi menjadi lebih kompleks.

Pemanfaatan tersebut akan membantu suatu pekerjaan seperti halnya pengolahan data lebih cepat, keputusan yang akan diambil lebih tepat, menghemat waktu dan biaya. Teknologi saat ini dibutuhkan di berbagai instansi, perusahaan, komunitas dan perguruan tinggi salah satunya adalah Politeknik Negeri Tanah Laut khususnya dalam bidang teknologi.

Politeknik Negeri Tanah Laut telah mengembangkan beberapa layanan aplikasi berbasis web. Dari semua layanan yang dibangun setiap pengguna harus memiliki akun disetiap layanan sehingga pengguna harus mengingat setiap akun untuk mengakses sistem dan untuk alasan keamanan biasanya pengguna mengganti passwordnya secara rutin.

Proses pergantian password ini akan memerlukan waktu yang cukup lama mengingat setiap perubahan yang dilakukan berbanding lurus dengan jumlah sistem yang ada (existing).

Oleh karena itu dibutuhkan suatu sistem yang dapat mengintegrasikan seluruh layanan aplikasi dan mengelola proses otentikasi dan otorisasi masing-masing sistem layanan. Otentikasi merupakan proses verifikasi untuk menentukan apakah seseorang berhak mengakses sistem aplikasi web atau tidak [1].

Cara yang paling sederhana adalah dengan menggunakan otentikasi login, dimana seorang pengguna memasukkan username dan password (credential), selanjutnya akan di verifikasi oleh sistem, apakah credential tersebut valid atau tidak valid, jika credential tersebut valid maka seorang pengguna boleh mengakses ke dalam sistem, jika tidak valid maka pengguna tidak berhak mengakses ke dalam sistem [2].

Proses otentikasi pada sistem terintegrasi memerlukan sebuah sistem tambahan yang menjadi penghubung antara sistem integrator dengan sistem layanan aplikasi. Sistem ini dapat menangani seluruh otentikasi setiap sistem aplikasi, sistem ini dikenal dengan Sistem Single Sign On (SSO). Sistem ini merupakan sebuah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Keuntungan dari sistem SSO adalah pengguna tidak perlu banyak mengingat username dan password serta memudahkan dalam pemrosesan data [3].

Single Sign On atau lebih dikenal dengan SSO merupakan sebuah platform identitas dan manajemen data pengguna yang memberikan pengelolaan, kemudahan dan kemanan pengguna. SSO memungkinkan pengguna untuk masuk sekali saja dan memiliki hak akses kesemua aplikasi yang telah mereka akses [1].

Gambaran dari SSO dapat dilihat pada gambar berikut:

Gambar 1. Diagram Blok Penelitian

Penelitian dalam hal pengembangan sistem otentikasi dan otorisasi menggunakan LDAP dan Radius sudah pernah dilakukan oleh beberapa peneliti diantara: Yuliansyah mengimplementasikan sistem otentikasi dan otorisasi untuk proses login multi aplikasi web berbasis PHP dengan mengoptimalkan penggunaan dari radius server. Hasil dari penelitian ini adalah pengguna pada beberapa aplikasi web berbasis PHP dapat diintegrasikan pengelolaannya dengan membangun sistem otentikasi dan otorisasi dengan radius server menggunakan aplikasi FreeRADIUS. Proses optimalisasi radius server sebagai sistem otentikasi dan otorisasi ini dapat membuat pengguna hanya akan memiliki satu akun tunggal untuk beberapa aplikasi yang berbeda [2].

Cloud Identity adalah produk Identitas sebagai Layanan (IDaaS) dan pengelolaan mobilitas perusahaan (EMM). Produk ini menawarkan layanan identitas dan administrasi endpoint yang tersedia di Google Workspace sebagai produk mandiri. Sebagai administrator, Anda dapat menggunakan Cloud Identity untuk mengelola pengguna, aplikasi, dan

perangkat dari satu lokasi terpusat, yaitu konsol Google Admin [4].

LDAP (Lightwieght Directory Access protocol) adalah Protokol yang digunakan untuk mengkases berbagai informasi dalam suatu direktori. LDAP dikembangkan atas dasar X.500 hanya saja lebih mudah dan mendukung TCP/IP. Walaupun penggunaannya berjumlah luas tapi LDAP yang merupakan Open Protocol sangat fleksibel karena bisa diimplementasikan untuk aplikasi seperti E-mail, Public Key dengan berbagai platform dan sistem operasi [5].

FreeRADIUS adalah RADIUS server yang Open Source. FreeRADIUS mendukung dengan semua protokol autentikasi dan dilengkapi web administrasi pengguna berbasis PHP yang disebut dialupadmin. FreeRADIUS dikembangkan oleh Alan Dekok dan Miquel Smoorenburg pada Agustus 1999. Sebelum mengembangkan FreeRADIUS, Miquel mengembangkan Cistron RADIUS server, namun tidak dikembangkan lagi. Seiring perkembangan waktu FreeRADIUS terus dikembangkan dan suport dengan banyak fitur selain support teks file juga support LDAP, MySQL, PostgreSQL, Oracle dan banyak fitur lainnya [6].

Muttaqin mengimplementasikan sistem otentikasi hotspot menggunakan LDAP dan RADIUS pada jaringan internet kampus Teknik Sistem Komputer Univeristas Diponegoro. Setiap server saling terintegrasi dan terkoneksi dengan jaringan internet kampus, Server RADIUS bisa melakukan akses ke database LDAP server menggunakan Radtest. Proses autentikasi hotspot menggunakan antarmuka login captive portal covachilli yang memblok jaringan local sehingga client tidak diijinkan masuk pada jaringan internet kampus sebelum login [3].

Qidri mengimplementasikan sistem otentikasi dan otorisasi untuk proses login ketika akan menggunakan internet. Implementasi sistem dibuat dalam aplikasi web berbasis PHP dengan mengoptimalkan penggunaan dari freeRadius. Pengguna dikelola dengan menggunakan aplikasi berbasis web dengan bahasa pemrograman PHP dan basis data MySQL [7].

Dari ketiga penelitian diatas dapat dilakukan inovasi untuk memaksimalkan pengembangan sistem otentikasi dan otorisasi dan disesuaikan dengan kebutuhan di Politeknik Negeri Tanah Laut (Politeknik Negeri Tanah Laut). Seluruh sivitas akademika Politeknik Negeri Tanah Laut memiliki akun email institusi yang berafiliasi dengan Google Suite Edu dimana otomatis memiliki cloud identity. Hal ini bisa dimanfaatkan sebagai data akun pengguna yang nantinya akan digunakan untuk login ke beberapa layanan aplikasi berbasis web termasuk layanan internet dikampus melalui suatu captive portal. Secure LDAP yang tersedia di Google Suite akan dijadikan penghubung ke server Radius. Radius akan menjadi integrator yang mengelola proses otentikasi dan otorisasi layanan aplikasi berbasis web dan layanan internet. Radius juga akan dintegrasikan dengan Mikrotik sebagai pengelola lalu lintas jaringan LAN dan internet di Politeknik Negeri Tanah Laut.

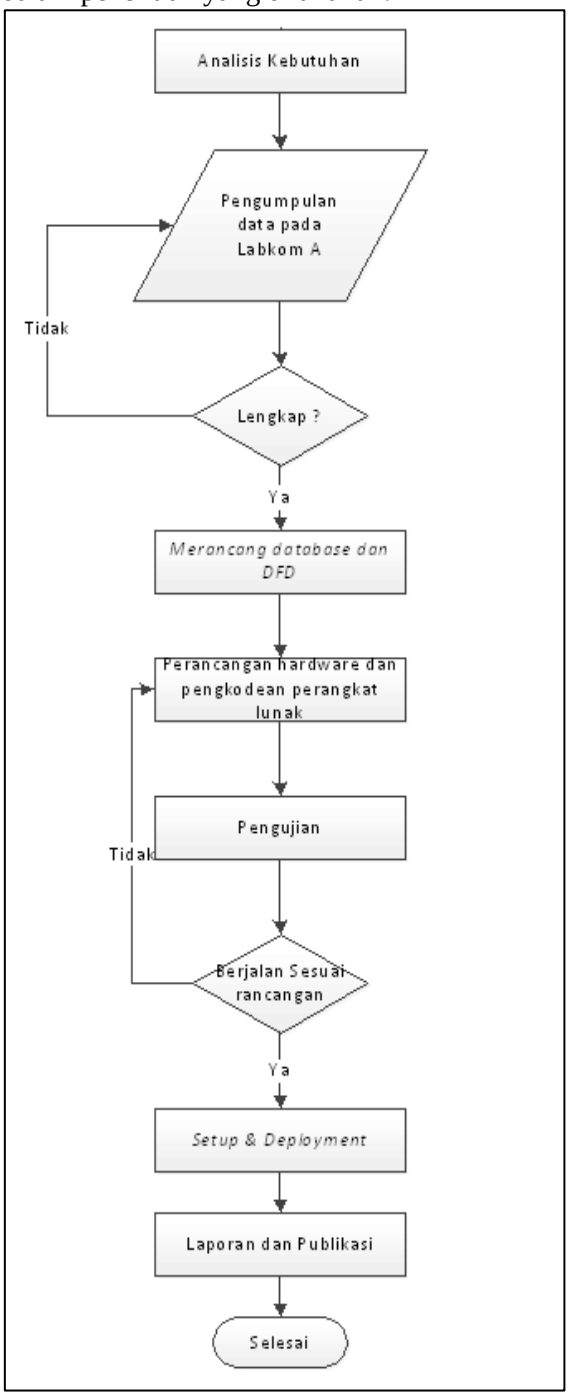
METODOLOGI

Metode penelitian yang dilakukan dalam penelitian ini meliputi tahapan-tahapan sebagai berikut.

1. Melakukan kegiatan analisis kebutuhan yang diperlukan dalam pengembangan sistem. Kegiatan ini meliputi identifikasi hardware berupa spesifikasi server yang akan digunakan.
2. Melakukan kegiatan pengumpulan data yang relevan terkait pengembangan sistem agar waktu pembangunan menjadi efektif dan efisien.
3. Selanjutnya setelah mendapatkan data yang lengkap, dimulailah merancang topologi sistem.
4. Setelah merancang topologi sistem, maka dilakukan proses konfigurasi server.
5. Tahapan berikutnya melakukan penulisan kode untuk proses otentikasi dan otorisasi.
6. Tahap berikutnya melakukan pengujian kinerja sistem, jika sesuai atau berhasil maka akan dilanjutkan ke tahap berikutnya. Jika belum sesuai, maka kembali ke tahap perancangan dan tahap pengkodean perangkat lunak untuk diperbaiki sampai berhasil.
7. Selanjutnya perangkat lunak yang sudah duji dan berhasil dilakukan Setup & deployment ke server produksi.
8. Tahapan terakhir yaitu membuat laporan dan pembuatan paper untuk publikasi sesuai perencanaan yang telah dibuat.

DOI: 10.47002/seminastika.v3i1.262

Berikut diagram blok tahapan kegiatan dalam penelitian yang dilakukan:



Gambar 2. Diagram Blok Penelitian

HASIL DAN PEMBAHASAN

Penelitian telah berhasil dilakukan dan diimplementasikan di pada website yang dimiliki oleh Politeknik Negeri Tanah Laut salah satunya https://kuesioner.politala.ac.id/. Berikut tampilan SSO yang dibangun:

Gambar 3. Tampilan Hasil Penelitian

Gambar 4. Tampilan Hasil Login

Gambar diatas menampilkan tampilan awal / *landing page* jika sebuah website yang telah dikonfigurasi diakses. Politeknik Negeri Tanah Laut memiliki beberapa website seperti:

1. https://kuesioner.politala.ac.id/
2. https://sipadu.politala.ac.id/
3. https://politala.ac.id/
4. https://aset.politala.ac.id/

Pengujian dilakukan secara langsung dengan mengakses website yang telah dikonfigurasi dan melakukan upaya login ke sistem. Pengujian berhasil dan pengguna dapat login ke sistem seperti tampak pada gambar 4.

Gambar 5. Tampilan Website Tanpa SSO

Gambar diatas merupakan salah satu website yang belum dilakukan konfigurasi dengan SSO sehingga username dan password login pada SSO tidak dapat digunakan pada website ini.

Dengan penerapan SSO akan mempermudah pengguna dalam mengkases website tersebut yaitu hanya menggunakan sebuah username dan password untuk berbagai website yang telah dikonfigurasi. Hal ini untuk menghindari pengguna dalam memliki

username dan password yang banyak dalam sebuah sistem yang telah terintegrasi.

KESIMPULAN

Kesimpulan dalam penelitian ini ialah telah berhasil dibangun dan diterapkan SSO dengan memanfaatkan *cloud identity* sebagai sumber data pengguna. Hal ini untuk mempermudah pengguna dalam login ke beberapa sistem yang terintegrasi cukup hanya menggunakan sebuah username dan password.

SARAN

Pengembangan selanjutnya dapat dilakukan dengan pengembangan otorisasi dan verifikasi login dengan akun gmail/google yang dimiliki pengguna. Hal ini akan sangat mempermudah sebab hampir semua pengguna internet saat ini memiliki akun google.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Politeknik Negeri Tanah Laut atas pendanaan penelitian yang diberikan dengan kontrak 023/PL-40.5/LT/2021 tahun .

DAFTAR PUSTAKA

[1] J. De Clercq, “Single sign-on architectures,” in *International Conference on Infrastructure Security*, 2002, pp. 40–58.

[2] H. Yuliansyah, “Dan Otorisasi Untuk Proses Login Multi Aplikasi Web,” *Semin. Nas. Inform. 2011*, vol. 2011, no. semnasIF, pp. 17–23, 2011.

[3] A. H. Muttaqin, A. F. Rochim, and E. D. Widianto, “Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer,” *J. Teknol. dan Sist. Komput.*, vol. 4, no. 2, p. 282, 2016, doi: 10.14710/jtsiskom.4.2.2016.282-288.

[4] Google, “Cloud Identity.” https://cloud.google.com/identity. (accessed Oct. 01, 2021).

[5] LDAP, “LDAP,” 2021. https://ldap.com/ (accessed Oct. 01, 2021).

[6] FreeRadius, “FreeRadius,” 2021. https://freeradius.org/ (accessed Oct. 01, 2021).

[7] S. Qidri, M. Asfi, R. Taufiq, and M. Hatta, “Pengelolaan Hak Akses User Jaringan Menggunakan Freeradius Untuk Login Jaringan,” *J. Sains dan Inform.*, vol. 6, no. 2, pp. 183–192, 2020.