

BAB II

KAJIAN LITERATUR

Bab II ini akan menjelaskan definisi, teori-teori dan penjelasan yang berkaitan dengan penelitian, serta memaparkan tentang penelitian terkait yang pernah dilakukan sebelumnya sebagai referensi. Tujuan dari melakukan kajian literatur pada penelitian ini yaitu untuk menggambarkan alur dari penelitian dan bagaimana penelitian tersebut terkait dengan penelitian-penelitian sebelumnya, serta untuk melakukan integrasi dan mengumpulkan secara ringkas mengenai teori-teori yang berkaitan dengan penelitian yang dilakukan. Kajian literatur pada penelitian ini dilakukan dengan mencari dari beberapa referensi berupa artikel, jurnal penelitian sebelumnya yang berkaitan dengan penelitian.

2.1 Tinjauan Pustaka

2.1.1 Autentikasi

Autentikasi merupakan sebuah proses usaha pengecekan identitas seorang pengguna sistem komunikasi pada proses login ke dalam sebuah sistem. Pengguna yang telah lolos pengecekan identitas adalah pengguna resmi pada sistem, orang yang memiliki otoritas atas sistem, atau mungkin aplikasi yang berjalan pada sistem. Penggunaan sistem otentikasi diharapkan dapat membentuk sebuah sistem khusus, yang hanya dapat dipergunakan oleh orang-orang yang memiliki hak guna. Ada perbedaan antara otentikasi dengan otorisasi; istilah otentikasi digunakan untuk pembuktian sebagai proses pengecekan identitas seorang pengguna, sedangkan otorisasi adalah proses pengecekan bahwa pengguna yang dikenal memiliki kekuasaan untuk melakukan tindakan tertentu[3].

dalam penggunaannya ada beberapa jenis autentikasi dalam proses validasi data pengguna, jenis-jenis autentikasi diantaranya ada **SFA** (*single factor authentication*), **2FA** (*two factor authentication*) dan **MFA** (*Multi factor authentication*).

a. *Single Factor Authentication*

SFA (single factor authentication) merupakan jenis autentikasi yang meminta pengguna untuk memasukkan ID pengguna. Kemudian proses autentikasi pun akan berjalan dengan meminta pengguna untuk memasukkan *password* yang tepat dan sesuai dengan ID pengguna.

b. *Two Factor Authentication*

(2FA) *two factor authentication* adalah proses autentikasi yang dikembangkan beberapa tahun setelah adanya **SFA** dan dimaksudkan untuk memperkuat keamanan. Pengguna akan divalidasi dengan beberapa pertanyaan terkait pengguna, kode unik **OTP** yang dikirimkan melalui *smartphone*, atau juga dengan wajah maupun sidik jari biometrik.

c. *Multi Factor Authentication*

Multi factor authentication (MFA) adalah jenis autentikasi yang mewajibkan pengguna untuk memverifikasi tiga jenis identitas, misalnya ID pengguna, sidik jari atau wajah, dan beberapa pertanyaan yang berhubungan dengan pengguna.

2.1.2 LDAP

Lightweight Directory Access protocol atau disebut dengan LDAP merupakan bagian dari internet protokol dan digunakan untuk mengakses berbagai informasi dalam suatu direktori. LDAP adalah pengembangan dari X.500 untuk mendukung kemudahan TCP/IP. LDAP bersifat open protokol dan fleksibel, artinya bisa diimplementasikan untuk berbagai aplikasi seperti *e-mail*, *public key* dengan berbagai platform dan sistem operasi. LDAP sendiri sudah dilengkapi SASL (*Simple Authentication and Security Layer*) untuk memeriksa dan memastikan apakah suatu *user* berhak dan diperbolehkan masuk atau tidak. Karena itulah LDAP juga banyak digunakan untuk '*single sign on*', yaitu dengan sekali *sign-on*, *user* dapat mengakses berbagai aplikasi yang telah disediakan. LDAP ini tidak hanya membaca informasi, tetapi juga bisa menambah dan mengupdate informasi yang ada *directory* tersebut [6].

1. Cara kerja LDAP

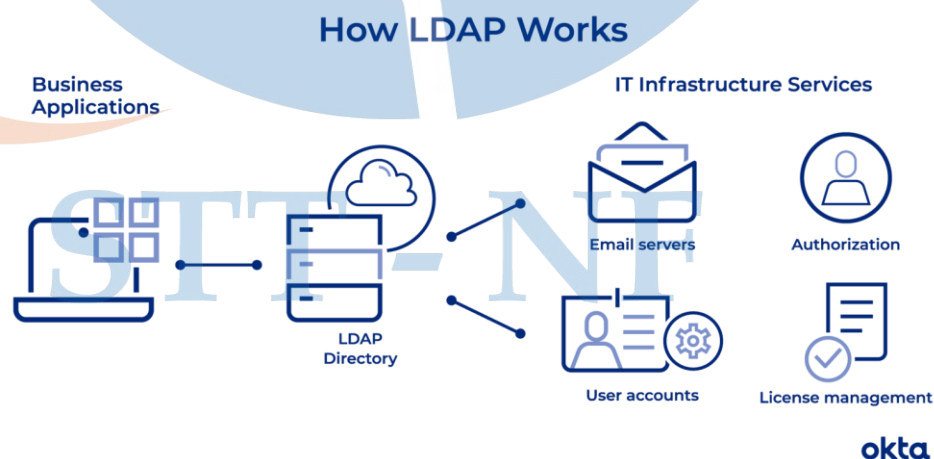
sebuah direktori telepon yang memiliki berbagai nama pelanggan yang diindeks secara alfabetis dengan nomor telepon dan alamat yang terkait adalah contoh

dari sebuah direktori. Struktur semacam ini dengan mudah dapat diimplementasikan menggunakan LDAP. Namun, protokol ini tidak terbatas hanya untuk mengakses informasi kontak tentang orang-orang. Hal ini dapat menemukan sumber daya berbagi pada jaringan seperti printer dan scanner, dan memungkinkan orang untuk menggunakan sumber daya dan layanan bersama lainnya menggunakan *password* tunggal [4].

Rata-rata karyawan di sebuah perusahaan terhubung dengan LDAP puluhan atau bahkan ratusan kali per hari. Orang tersebut bahkan mungkin tidak mengetahui bahwa koneksi telah terjadi meskipun langkah-langkah untuk menyelesaikan query rumit dan kompleks.

Kueri LDAP biasanya melibatkan:

- **Session connection.** Pengguna terhubung ke server melalui port LDAP.
- **Request.** Pengguna mengirimkan kueri, seperti pencarian email, ke server.
- **Response.** Protokol LDAP menanyakan direktori, menemukan informasi, dan mengirimkannya ke pengguna.
- **Completion.** Pengguna memutuskan sambungan dari port LDAP



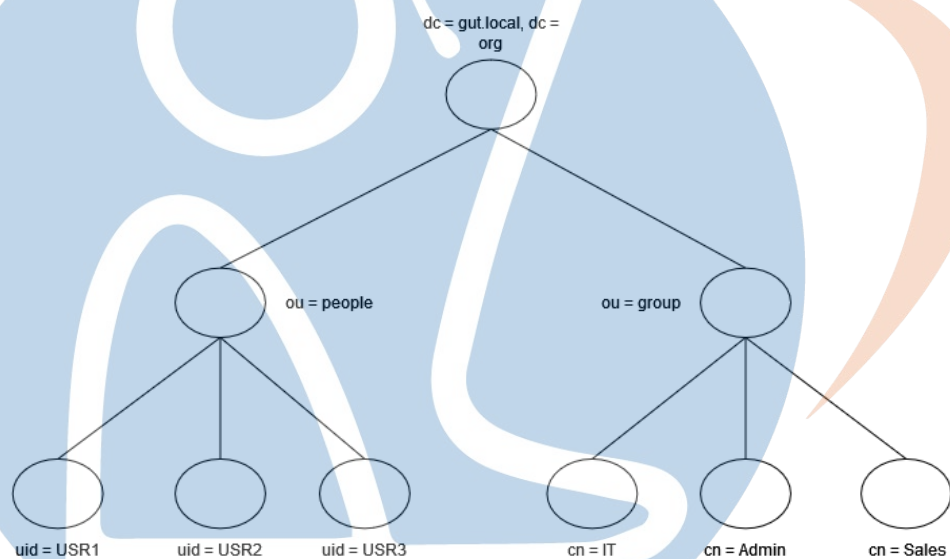
Gambar 2.1 Cara Kerja LDAP

2. Fungsi LDAP

LDAP adalah TCP / IP berbasis protokol internet yang digunakan oleh program email dan beberapa aplikasi lain untuk mencari dan mengambil informasi dari sebuah direktori disimpan pada sebuah server. Direktori adalah repository menyimpan data potongan identik dari informasi dalam urutan hierarkis dan logis [6].

3. Struktur Database

Struktur database pada suatu *directory service* adalah hierarki seperti yang di tunjukkan pada gambar berikut:



Gambar 2.2 struktur database

Secara prinsip struktur database pada suatu *directory service* adalah hierarki seperti yang ditunjukkan pada gambar di atas. Suatu *directory service* akan memiliki item yang di jadikan sebagai root. Untuk sebuah titik root, secara umum di tunjukkan dengan suatu atribut dc (*Domain Component*) atau ou (*Organization Unit*). Kemudian pada titik daun (leaf) biasanya akan berisi item dengan atribut uid (*User ID*) ataupun cn (*Common Name*). *Directory service* biasanya menyimpan informasi dalam bentuk struktur tree yang dinamakan *Directory Information Tree* (DIT). Setiap titik pada DIT diberi suatu alamat, yang disebut sebagai DN (*Distinguish Name*). Contoh Pengalamatan untuk *user*

USR1 adalah “dn=uid=USR1,ou=personal,dc=gut.local,dc=org”. Konsep seperti inilah yang di gunakan oleh direktori LDAP.

2.1.3 Fortinet

Fortinet merupakan *provider* keamanan jaringan ternama yang sudah diakui oleh *Gartner* sebagai leader *Unified Threat Management* (UTM) kelas dunia termasuk pada *enterprise firewall*. Berawal dari solusi FortiGate yang merupakan solusi best seller dari fortinet. FortiGate enterprise firewall memberikan solusi pengurangan kompleksitas dan peningkatan keamanan jaringan secara keseluruhan melalui visibilitas penuh ke aplikasi, perangkat, pengguna serta ancaman pada jaringan. Hal ini dilakukan untuk meningkatkan kemampuan penerapan perlindungan ancaman dimana saja pada jaringan [7].

Fortigate menjadi platform keamanan dengan perpaduan *ASIC Accelerated*, kecepatan respon terhadap multi ancaman secara terpadu, serta memberikan update terbaru dengan fitur intelijen ancaman kelemahan keamanan yang mendalam. Sistem fortinet mengintegrasikan fitur terluas dalam teknologi keamanan termasuk Antivirus, Intrusi (IPS), VPN, Antispam, Wireless Controller, WAN Accelerator serta pengendalian aplikasi yang dapat digunakan secara individual. fortigate sudah di tambahkan fitur tanggapan secara realtime berdasarkan threat intelligence yang mampu melindungi titik kerentanan pada semua jaringan. Salah satu fitur yang sangat mengesankan yakni layanan audit ataupun compliance yang terintegrasi yang dapat membantu memperbaiki *cybersecurity*. Sebagai teknologi keamanan andalan utama, Fortinet memiliki sistem manajemen yang luas, analisa yang akurat, serta solusi perlindungan endpoint yang mampu meningkatkan fleksibilitas penggunaan produk [7].

1. Fleksibilitas Manajemen Yang Ditawarkan Fortinet

Fleksibilitas manajemen ini akan sangat membantu dalam proses pembaharuan perangkat yang ada dalam kantor. Hal ini akan meningkatkan efisiensi waktu tanpa harus melakukan pembaruan satu per satu perangkat keamanan pada perangkat.

Meskipun hanya melakukan setting keamanan perangkat saat pertama kali, FortiGate menjamin keamanan jaringan perangkat secara menyeluruh, baik sebagai gateway, VPN, router firewall, antivirus dan lainnya. Dan yang paling mengesankan adalah, FortiGate memberikan akses pemantau ataupun monitoring perangkat melalui internet browser atau baris command.

2. UTM Fortinet Yang Diberikan

Fortinet menawarkan fitur UTM sebagai fasilitas penanganan masalah jaringan. Fitur yang ditawarkan yakni firewall, web filtering, antivirus dan routing, intrusion prevention system (IPS) pada satu paket perangkat keras fortinet yang ditawarkan. Saat ingin menggunakan perangkat FortiGate, maka sistem akan berjalan secara bersamaan tanpa melakukan pengaturan yang rumit. Layanan jaringan, keamanan jaringan maupun keamanan aplikasi. Namun jangan khawatir, Fortigate memberikan preferensi fleksibilitas layanan yang akan digunakan.

3. Fitur Virtual Domain (VDoms)

Fortinet memberikan akses ke berbagai perusahaan melalui administrator yang berbeda, dan perlu Anda ketahui bahwa ini menggunakan unit fisik yang sama. Tujuan fitur ini untuk memastikan bahwa masing-masing konfigurasi yang spesifik terjaga dan tidak memiliki ancaman keamanan.

4. Proteksi FortiGuard

Fortiguard merupakan jasa support yang disediakan khusus sebagai layanan support lanjutan untuk keamanan jaringan komputer. Fasilitas support ini mempunyai database jutaan situs yang dikelompokkan secara berbeda. Biasanya, staf yang bertugas pada support fortiguard ini memiliki wewenang penuh dalam melakukan monitoring dan pemblokiran situs yang dianggap sebagai ancaman. FortiGuard dapat digunakan untuk mengontrol pemakaian bandwidth internet, pengaturan pemakaian akses internet yang dapat disesuaikan dengan kebijakan perusahaan.

2.1.4 WIRELESS

Teknologi *wireless* saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Computer, notebook, dan telepon seluler (handphone) mendominasi pemakaian teknologi *wireless*. Penggunaan teknologi *wireless* yang diimplementasikan dalam suatu jaringan lokal sering dinamakan WLAN (*Wireless Local Area Network*). Namun perkembangan teknologi *wireless* yang terus berkembang sehingga terdapat istilah yang mendampingi WLAN seperti WMAN (Metropolitan), WWAN (Wide), dan WPAN (Personal / Private) (Rifky Wahyu Pratama 2019) [3].

2.1.5 Active Directory

Active Directory adalah layanan direktori yang dimiliki oleh sistem operasi jaringan Microsoft Windows server, *Active Directory* terdiri atas basis data dan juga layanan direktori. Basis data yang dimiliki oleh *Active Directory* menyimpan segala sumber daya yang terdapat di dalam jaringan, seperti halnya komputer yang telah bergabung ke sebuah domain, daftar akun pengguna dan kelompok pengguna, folder yang di-share, dan lain-lain. Sementara itu, layanan direktori yang dimilikinya membuat informasi yang disimpan di dalam basis data dapat diakses oleh pengguna dan aplikasi. *Active Directory* sebenarnya merupakan implementasi dari protokol *Lightweight Directory Access Protocol* (LDAP) [5].

Peranan Utama *Active Directory* adalah menyediakan sarana untuk melakukan administrasi jaringan secara terpusat baik di level domain maupun lintas domain, selama antar domain tersebut masih berada dalam satu forest. Struktur logika *Active Directory* dibagi menjadi beberapa bagian, struktur ini yang membentuk direktori pada *Active Directory* yang berguna untuk memusatkan basis data dalam perusahaan. Berikut merupakan struktur yang terdapat dalam *Active Directory* (Rifky Wahyu Pratama 2019):

a. *Object*

Object merupakan konsep dasar dari struktur Logical *Active Directory*. *Object*

bisa berupa *user*, komputer, atau printer yang berada didalam jaringan perusahaan.

b. *Organization Unit (OU)*

Organization Unit merupakan suatu wadah yang mengelompokkan *object* ke dalam unit-unit administrasi sesuai dengan kebutuhan organisasi.

c. *Domain*

Domain adalah pengelompokan logis dari komputer dan pengguna untuk tujuan administrasi jaringan.

d. *Tree*

Tree adalah adalah suatu pengelompokan atau pengaturan secara hirarki dari satu atau lebih *domain*.

e. *Forest*

Forest merupakan kumpulan dari pohon atau *tree domain*. Ketika melakukan instalasi, *forest* secara otomatis dibuat implementasi seluruh *Active Directory*.

2.2 PT XYZ

PT.XYZ adalah perusahaan yang bergerak dibidang penjualan kamera profesional yang beralamatkan di Gunung Sahari Jakarta Pusat, PT.XYZ juga tak hanya sebagai penjual kamera saja, tetapi juga lengkap dengan aksesoris dan perangkat audio profesional, PT.XYZ juga adalah sebagai distributor dari salah satu kamera ternama yaitu FUJIFILM.

Sebagai perusahaan yang bergerak di bidang pemasaran tentunya PT.XYZ memiliki cukup banyak karyawan yang membantu semua proses pemasaran, baik itu bidang Administrasi, Marketing dan Teknologi Informasi.

2.3 Tinjauan penelitian terkait

Table 2.1 Penelitian Terkait

NO	Judul Penelitian	Peneliti	Tahun	Kesimpulan
1	Implementasi Single Sign-On Berbasis Active Directory Sebagai Basis Data dan Layanan Direktori	Salman Farizy	2018	AD sangat diperlukan dalam infrastruktur untuk menyimpan semua konfigurasi, baik itu user, group, aplikasi, policy dan masih banyak yang lainnya secara terpusat. Keamanan Sistem Informasi dapat terjaga dan terpantau, dari penyalahgunaan dari user yang tidak bertanggung jawab.
2	Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet <i>Wireless</i> Prodi Teknik Sistem Komputer	Ahmad Herdinal Muttaqin	2016	Proses Autentikasi Hotspot menggunakan antarmuka <i>captive portal</i> yang memblokir jaringan lokal sehingga <i>client</i> tidak diizinkan masuk pada jaringan internet kampus sebelum <i>login</i> .
3	Implementasi Sistem Autentikasi <i>User</i> Menggunakan <i>Radius Server</i> dan <i>Active Directory</i> pada Jaringan <i>Wireless</i> di PT. Kudo Teknologi Indonesia	Rifky Wahyu Pratama	2019	Implementasi berhasil dilakukan sehingga pengguna dapat melakukan koneksi menggunakan username dan password yang terdaftar pada active directory
4	Penerapan Autentikasi Terpusat Untuk	Amin Ma'ruf	2022	Rancangan Penerapan Autentikasi Terpusat Untuk Keamanan Jaringan <i>Wireless</i>

	Keamanan Jaringan <i>Wireless</i> Menggunakan Perangkat Fortinet Terintegrasi Dengan Windows Active Directory Pada PT. XYZ		Menggunakan Perangkat Fortinet Terintegrasi Dengan Windows Active Directory Pada PT.XYZ telah berfungsi sesuai dengan konfigurasi yang telah dirancang. Untuk tingkat efektifitasnya sangat efektif dibuktikan dengan hasil uji efektifitas
--	--	--	---

Penelitian ini disusun berdasarkan kesamaan latar belakang dari penelitian yang ada sebelumnya dan menjadi rujukan bagi penulis untuk melakukan penelitian di PT.XYZ, yaitu dari Rifky Wahyu Pratama pada tahun 2019 dengan judul Implementasi Sistem Autentikasi *User* Menggunakan *Radius Server* dan *Active Directory* pada Jaringan *Wireless* di PT.Kudo Teknologi Indonesia, kesamaan dengan penelitian tersebut adalah penggunaan *Active Directory* sebagai databasanya sedangkan hal yang membedakan adalah pada penggunaan routernya, pada penelitian Rifky Wahyu digunakan mikrotik sedangkan penulis menggunakan Fortinet.

STT - NF