I. PENDAHULUAN

1.1 Latar Belakang

PT. XYZ merupakan salah satu perusahaan yang bergerak dibidang energi. Pada perusahaan tersebut terdapat lima satuan kerja, diantaranya adalah kendali produk, perawatan, keselamatan dan kesehatan kerja (K3) , operasi, dan sumber daya manusia (SDM) yang membawahi beberapa divisi untuk mendukung serta menjalankan segala operasional kegiatan perusahaan. Masing – masing divisi kerja akan melaksanakan tugasnya sesuai dengan pembagian kerja yang telah ditentukan.

Pada proses kegiatan operasional perusahaan, masing – masing divisi memerlukan koneksi jaringan wireless untuk terhubung ke internet. Divisi keuangan membutuhkan koneksi internet untuk mengirim *email* untuk urusan internal dan eksternal. Divisi penunjang operasi harus terhubung ke aplikasi VNC agar dapat memonitoring berjalannya mesin yang terintegrasi dengan sistem *automation*. Seluruh karyawan perusahaan juga membutuhkan koneksi internet untuk mengakses aplikasi perusahaan guna keperluan pekerjaan lainnya. Saat ini jaringan internet yang ada di dalam perusahaan memiliki *bandwith* 150 Mbps dengan tipe *dedicated* dan terdapat 6 VLAN yang berguna untuk *user* dan perangkat operasional perusahaan.

Untuk terhubung ke dalam jaringan perusahaan terdapat sistem keamanan berbasis WPA2-PSK sehingga *user* diwajibkan memasukan *password* wifi perusahaan. WPA2-PSK merupakan metode keamanan jaringan *wireless*, WPA2-PSK menggunakan dua tipe enkripsi yaitu *Advanced Encryption Standard* (AES) dan *Temporal Key Integrity Protocol* (TKIP) (Michael dkk., 2021). Metode keamanan ini mencegah tim IT dari memperoleh informasi terkait identitas *user* yang tengah terhubung dalam jaringan. Meskipun demikian, semakin meningkatnya jumlah pengguna yang ingin mengakses jaringan, muncul isu - isu keamanan yang timbul seiring kondisi tersebut menjadi tidak terhindarkan. Salah satu isu yang muncul adalah kesulitan dalam mengidentifikasi status *user* yang berupaya mengakses jaringan.

Hambatan ini muncul dikarenakan metode otentikasi yang diterapkan untuk akses ke dalam jaringan perusahaan bergantung pada metode WPA2-PSK.

Selain permasalahan dari segi keamanan jaringan, dengan pengunaan *key security* tersebut *user* selain karyawan dapat terhubung ke jaringan menggunakan perangkat pribadi. Dampak dari kegiatan tersebut akan membuat IP *lease* yang ada pada DHCP *Server* menjadi penuh. Permasalahan yang akan timbul dari hal tersebut adalah perangkat perusahaan yang ingin terhubung ke dalam jaringan menjadi terhambat akibat tidak mendapatkan IP *address* dari DHCP *server* yang seharusnya di gunakan untuk kegiatan pekerjaan.

Sebagai salah satu solusi untuk memperbaiki sistem autentikasi yang ada pada saat ini, terdapat sistem keamanan yang dapat dimanfaatkan seperti RADIUS. Sistem RADIUS akan digunakan sebagai salah satu metode keamanan yang akan diterapkan pada tugas akhir ini. RADIUS merupakan sebuah standar keamanan komputer yang penerapannya ditujukan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun *user* secara terpusat (Darmadi, 2018). Berdasarkan latar belakang yang telah diuraikan penulis tertarik untuk melakukan pengkajian lebih dalam dengan merancang "Autentikasi *User* Dengan Metode *Single Sign-On* Berbasis *Windows Active Directory* Pada PT. XYZ".

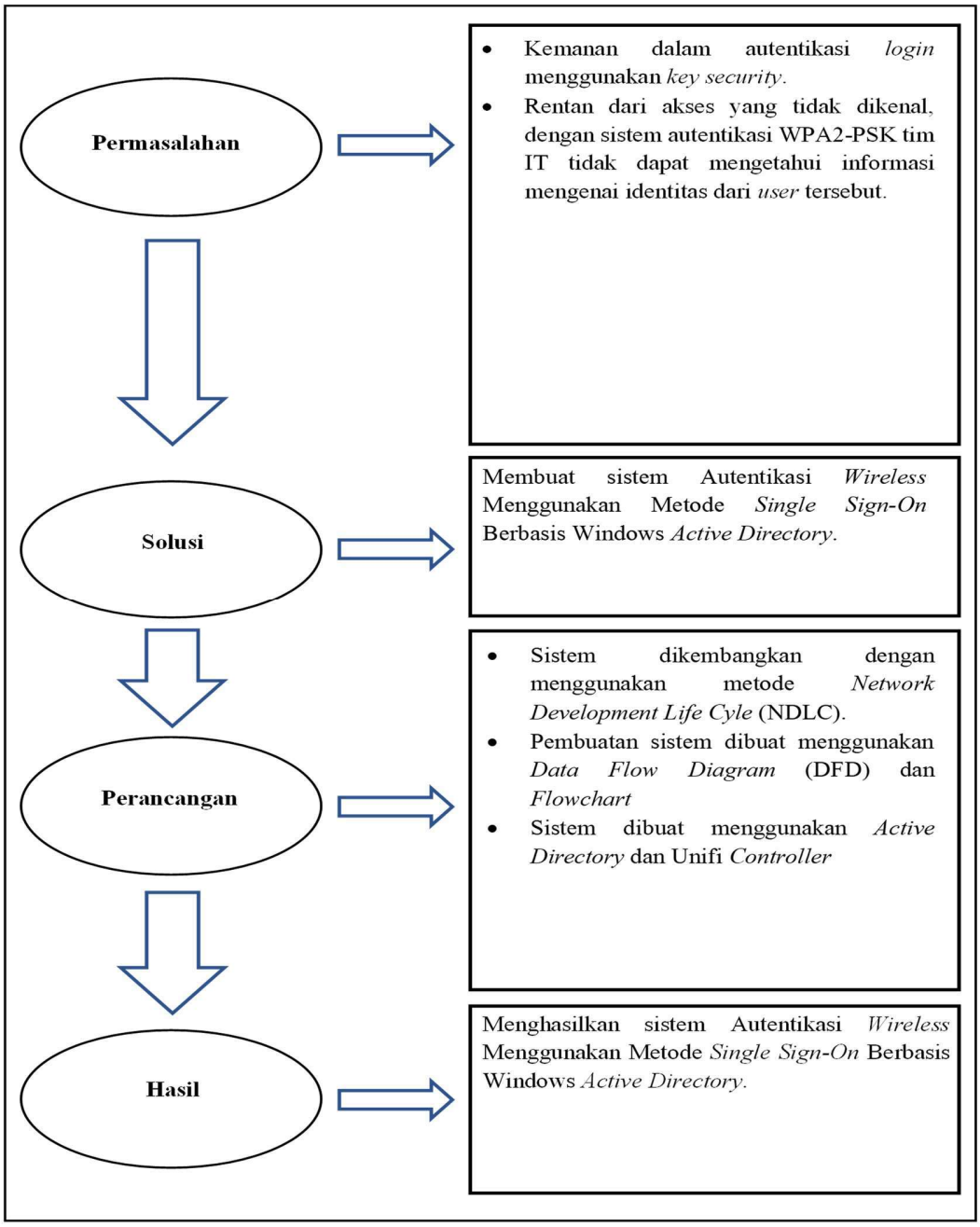
1.2 Tujuan

Tujuan tugas akhir ini adalah menghasilkan sistem autentikasi *user* dengan metode *single sign-on*. Sistem dijalankan untuk menghindari ancaman pada sistem keamanan jaringan. Kendala seperti lupa *password* ketika ingin terhubung ke dalam jaringan atau IP *addres* pada DHCP *server* yang penuh akan teratasi dengan adanya sistem autentikasi metode *single-sign on*.

1.3 Kerangka Pemikiran

Salah satu upaya untuk melindungi jaringan serta mempermudah *user* untuk dapat melakukan *login* yang tersentral pada jaringan adalah dengan membuat sistem

autentikasi yang terintegrasi dengan *database Active Directory*. Sistem autentikasi yang aman dan terintegrasi akan meningkatkan kenyamanan *user* dalam menggunakan jaringan.



Gambar 1. Kerangka Pemikiran

1.4 Kontribusi

Pada pembuatan sistem Autentikasi *User* Dengan Metode *Single Sign-On* Berbasis *Windows Active Directory* Pada PT. XYZ diharapkan dapat memberikan manfaat kepada tim IT serta karyawan yang ada karena sitem ini akan menjadi solusi untuk memperbaiki sistem keamanan yang ada. Manfaat tersebut akan dirasakan oleh pihak berikut :

1. Tim IT

   Adapun Manfaat yang didapatkan tim IT terhadap sistem autentikasi ini yaitu :

   a. Membantu tim IT dalam melakukan monitoring *user* yang masuk ke dalam jaringan perusahaan.
   b. Membantu tim IT untuk menghindari terjadinya IP *lease* DHCP *server* yang penuh.
   c. Membantu dalam melindungi jaringan dari akes yang tidak dikenal.

2. Karyawan

   Adapun manfaat yang didapatkan karyawan terhadap sistem autentikasi ini yaitu:

   a. *User* tidak perlu lagi khawatir ketika lupa *password* untuk terhubung ke dalam jaringan *wireless*.
   b. *User* akan lebih mudah ketika ingin masuk kedalam jaringan dikarenakan metode *single sign-on.*

II. TINJAUAN PUSTAKA

2.1 Autentikasi *Single Sign On*

Autentikasi merupakan sekian dari banyaknya cara untuk memverifikasi keaslian, yaitu dengan cara membuktikan terhadap informasi mengenai identitas *user* ketika ingin masuk ke dalam sebuah sistem (Syarif Aziz, 2021). *Single Sign-On* (SSO) merupakan sebuah metode dalam sistem agar melakukan verifikasi yang memberikan kesempatan bagi *user* untuk dapat melakukan satu kali *login* ke beberapa sistem atau aplikasi sekaligus. Menurut (Fathurrahmani, dkk., 2021) *Single Sign-On* memiliki keunggulan dikarenakan dengan sistem tersebut *user* tidak perlu mempunyai *username* ataupun *password* yang lebih dari satu agar bisa mempercepat proses akses ke dalam sistem.

2.2 *Wireless*

Wireless merupakan sebuah teknologi yang identik dengan sistem jaringan dimana komputer dapat saling terhubung tanpa menggunakan media fisik seperti kabel, hal ini memberikan fleksibilitas dan kepraktisan dalam melakukan mobilitas kegiatan dengan presentase yang tinggi (Rusdan & Sabar, 2020).

2.2.1 *Controller*

Menurut (Ruseno, 2018) *controller* adalah komponen yang memanajemen interaksi antara bagian model dan bagian tampilan, *controller* juga memiliki peran untuk menerima perintah dan data dari *user* untuk ditindak lanjuti tindakan apa yang perlu dilakukan oleh sistem. Pada umumnya *controller* akan menerima perintah dan memproses perintah tersebut untuk diteruskan ke sistem, setelah menerima perintah sistem akan menjalankan kondisi yang diinginkan oleh *user.*

2.2.2 IP *address* dan DHCP *server*

Dynamic Host Control Protocol atau biasa disingkat dengan DHCP merupakan satu diantara protokol jarigan yang cukup populer untuk digunakan pada sebuah

konfigurasi *host* dalam membangun infrastruktur jaringan antara *client* dan *server* (Ariyadi, 2018). IP *address* merupakan kumpulan angka yang berderet pada sebuah perangkat yang terhubung dengan sebuah jaringan internet (Sudirman, 2022). IP *address* memiliki rangkaian angka yang unik untuk digunakan sebagai identitas dan pembeda pada setiap perangkat yang menggunakan sebuah protokol jaringan.

2.3 Sistem Operasi *Windows* dan *Server*

Sistem Operasi *Windows* adalah salah satu dari banyaknya jenis sistem operasi yang umumnya ada pada perangkat komputer maupun laptop. Sistem operasi *Windows* berada di bawah naungan perusahaan Microsoft milik Bill Gates, *Windows* pertama kali diluncurkan pada tahun 1985 dengan tampilan *user interfaces* berbasis *Graphical User Interfaces* (GUI). *Windows* merupakan sistem operasi yang dikembangkan oleh Microsoft dengan mengimplementasikan GUI (*Graphical User Interfaces*) sebagai antar mukanya (Sumarto, 2014). *Server* adalah sebuah sistem komputer yang mempunyai peranan khusus yaitu melakukan manajemen penyimpanan data. Perangkat *serve*r berbeda dengan perangkat biasa yang umumnya digunakan oleh *user*, sebuah *server* harus di dukung dengan spesifikasi yang memumpuni mulai dari prosesor yang memiliki durabilitas yang kuat dan RAM yang besar, serta memiliki sistem operasi khusus (Ruli Dimas Prakoso, 2017).

2.4 *Active Directory* dan RADIUS

Active Directory merupakan sebuah tempat penyimpanan layaknya *database* yang melakukan manajemen distribusi menggunakan fasilitas direktori untuk dapat diterapkan diantara semua sistem kontrol domain pada jaringan (Pratama, 2019). *Active Directory* dapat ditemui di sistem operasi seperti *Windows Server,* didalamnya *Active Directory* akan berdampingan dengan *Domain Controll*er untuk digunakan sebagai manajemen *user* beserta *rules* dan akses *user* baik secara per individu maupuan dalam sebuah grub yang tergabung dengan *domain* yang sama. Pada pendapat yang dikemukakann oleh (Haeruddin & Pangaribuan, 2021) *Active Directory* dapat mempermudah administrator untuk memanajemen serta melakukan pemeliharaan hak

akses keseluruhan *user* berdasarkan keinginan perusahaan. RADIUS merupakan sebuah singkatan dari *Remote Authentication Dial In User Service* adalah sejenis *server* yang diperuntungkan untuk menjalankan perintah *service authentication*, dan *accounting* (AAA) pada sebuah jaringan. Radius adalah sebuah protokol pada keamanan jaringan komputer yang dikonfigurasi untuk kebutuhan otentikasi, otorisasi, dan registrasi akun *user* secara terpusat ketika ingin mengakses jaringan (Haeruddin & Pangaribuan, 2021).

2.5 NPS (*Network Policy Server*) dan CA (*Certification Authority*)

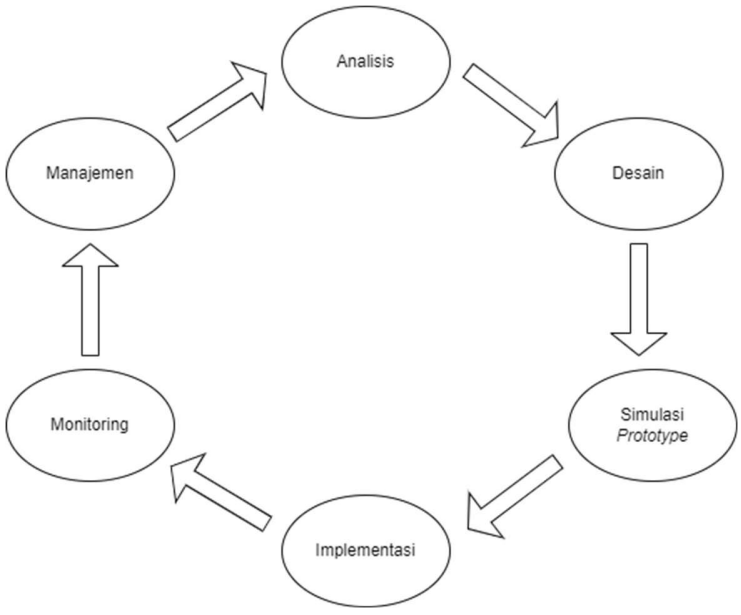
NPS bisa diartikan sebagai sebuah metode terapan RADIUS *server* dan *proxy* versi microsoft, sebagai *server* RADIUS, NPS dapat menjadi sistem terpusat untuk autentikasi dan otorisasi pada berbagai macam jaringan diantarnya *wireless* dan VPN (Andriani, 2007). CA merupakan sebuah organisasi yang meninjau dan memanajemen berbagai peraturan yang berkaitan dengan regulasi kepercayaan pada kegiatan elektronik (Cahyadi, 2009). CA memiliki fungsi sebagai pihak ketiga yang dapat dipercaya serta memberikan dan meninjau sertifikat elektronik lalu menyediakan layanan keamanan yang dapat digunakan oleh *user* ketika melaksanakan pertukaran informasi.

2.6 *Network Development Life Cyle*

Network Development Life Cyle atau biasa disingkat dengan sebutan NDLC adalah sebuah metode yang bermanfaat untuk pengembangan jaringan yang ada dengan menjalankan beberapa proses seperti analisis, desain, simulasi, implementasi, monitoring, sampai manajemen (Sanjaya & Setiyadi, 2019). Berikut ini adalah penjelasan mengenai masing – masing tahapan yang ada pada metode NDLC menurut (Sanjaya & Setiyadi, 2019) :

1. Analisis, tahapan yang akan dilakukan adalah mengumpukna data yang akan di gunakan sebagai dasar dari perumusan masalah untuk mengatasi kendala yang ada.

2. Desain merupakan tahapan kedua pada metode NDLC, di dalamnya terjadi sebuah proses mengelola data – data yang dikumpulkan untuk membuat desain dari topologi autentikasi yang akan di kerjakan.
3. Simulasi protoype merupakan tahapan pengembangan dengan membuat model sistem dengan bantuan tools.
4. Impelementasi merupakan tahapan yang akan menjadi kegiatan utama di karenakan penulis akan menerapkan segala hal yang telah di rancang sebelumnya.
5. Monitoring merupakan tahapan yang dilaksanakan setelah implementasi, tahapan ini cukup penting dikarenakan akan memantau apakah jaringan dan komunikai telah berjalan baik serta sesuai dengan tujuan penulis.
6. Manajemen adalah tahapan yang membutuhkan perhatian khusus hal ini terjadi dikarenakan kebijakan untuk mengatur agar sistem yang dibuat dan berjalan dapat sesuai dengan harapan yang diinginkan.



Gambar 2. *Network Development Life Cyle*

2.7 Jurnal Terkait

Jurnal terkait memiliki tujuan sebagai sumber untuk mengetahui perbedaan penelitian yang akan dilaksanakan dengan penelitian sebelumnya. Penelitian sebelumnya merupakan penelitian yang memiliki keterkaitan dengan penelitian saat ini. Berikut adalah beberapa penelitian yang diperoleh mengenai sistem autentikasi *user* dengan *single sign-on* :

1. Jurnal yang disusun oleh Musliyana dan kawan - kawan, (2016) yang memiliki judul "Peningkatan Sistem Keamanan Otentikasi *Single Sign On* (SSO) Menggunakan Algoritma AES dan *One-Time Password* Studi Kasus: SSO Universitas Ubudiyah Indonesia". Penelitian ini di latar belakangi oleh sistem SSO UUI yang berjalan masih menggunakan protokol HTTP, hal ini menyebabkan kerentanan terhadap berbagai jenis serangan karena data dikirim dalam bentuk *plaintext* tanpa terlindungi dengan enkripsi. Dari latar belakang tersebut penelitian ini menghasilkan sistem keamanan pada SSO dengan menggunakan algoritma AES dan *one-time password* yang tentunya lebih aman dibandingkan sistem sebelumnya.
2. Jurnal yang disusun oleh Putri dan kawan - kawan, (2019) yang memiliki judul "Sistem Otentikasi *Login* dengan *Single Sign-On* untuk Mengakses Banyak Sistem". Penelitian ini di latar belakangi oleh sistem otentikasi pengguna yang umumnya masih menggunakan banyak akun untuk dapat mengakses ke dalam layanan aplikasi yang dinginkan. Dari latar belakang tersebut penelitian ini menghasilkan sistem otentikasi *login* dengan *single sign-on* serta dapat mempermudah pengguna untuk mengakses aplikasi yang berbeda hanya dengan satu akun yang sama.
3. Jurnal yang disusun oleh Mahedy, (2022) yang memiliki judul "Pengembangan Sistem Autentikasi *Hotspot* Terpusat Berbasis Teknologi *WEB Service* Di Universitas Pendidikan Ganesha". Penggunaan sistem *key security* pada jaringan *wireless* kurang fleksibel ketika melakukan distribusi *key* enkripsinya. Dari latar belakang tersebut penelitian ini memberikan sebuah hasil yaitu akun *user* pengguna *hotspot* pada Universitas Pendidikan Ganesha akan tersimpan pada

database mysql dengan sistem terpusat lalu akan diproses dengan sinkronasi ke aplikasi SSO (*Single Sign-On*) yang dimiliki Universitas.

Berdasarkan uraian di atas yang membahas mengenai jurnal terkait berikut merupakan rangkuman dari jurnal terkait yang digunakan dalam pembuatan sistem autentikasi *single sign-on* yang dapat dilihat pada Tabel 3.

Tabel 1. Jurnal Terkait

Nama dan Tahun	Judul	Metode Pengembangan Sistem	Metode Pengumpulan Data	Hasil
Zuhar Musliyana, Teuku Yuliar Arif, dan Rizal Munadi (2016)	Peningkatan Sistem Keamanan Otentikasi *Single Sign On* (SSO) Menggunakan Algoritma AES dan *One-Time Password* Studi Kasus: SSO Universitas Ubudiyah Indonesia	Metode Penelitian Kuantitatif	Wawancara dan Observasi	Sistem keamanan pada SSO dengan menggunakan algoritma AES dan *one-time password* yang tentunya lebih aman dibandingkan sistem sebelumnya.
Theta Dinnarwaty Putri, Winarno Sugeng, dan Resi Katri (2019)	Sistem Otentikasi *Login* dengan *Single Sign-On* untuk Mengakses Banyak Sistem	Metode Penelitian Model Prototipe	Observasi	Sistem otentikasi *login* dengan *single sign-on* yang dapat mempermudah pengguna untuk mengakses aplikasi yang berbeda hanya dengan satu akun yang sama.

Kadek Surya Mahedy (2022)	Pengembangan Sistem Autentikasi *Hotspot* Terpusat Berbasis Teknologi *WEB Service* Di Universitas Pendidikan Ganesha	Metode Penelitian Paradigma *Prototyping*	Observasi	Sistem otentikasi *login* dengan *single sign-on* dapat digunakan sebagai fitur untuk kontrol pada tiap *user* dan *user* dapat selalu sinkron dengan antar sistem yang sudah ada maupun masih di kembangankan di Undiksha.