Implementasi WPA2 Enterprise dan LDAP Dalam Membangun Sistem Informasi Kehadiran Karyawan

IGL. Putra Eka Prismana[a,*], Ginanjar Setyo Permadi[b], Wahyu Khamdani[c]

[a]Jurusan Pendidikan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Surabaya, Surabaya - Indonesia
[b]Jurusan Manajemen Informatika, Fakultas Teknologi Informasi, Universitas Hasyim Asy'ari, Jombang – Indonesia
[c]Jurusan Teknik Informasi, Fakultas Teknik, Universitas Negeri Surabaya, Surabaya - Indonesia

Naskah Diterima : 30 Agustus 2020; Diterima Publikasi : 6 Desember 2020
DOI: 10.21456/vol10iss2pp195-202

Abstract

Technological developments have a positive effect on agencies and companies, one of which is the innovation of employee attendance registration using the internet network media. Employee attendance system model using internet network will certainly make it easier to control employee attendance. The internet network is an important part of every agency in helping its performance and can also be used as an attendance system. WPA2 Enterprise implementation is used as authentication using the provided email and password. Devices that have been connected to the network will automatically be recorded in the employee attendance system. The implementation of WPA2 Enterprise requires freeradius assistance in processing authentication data from employees which will then be verified again through LDAP, in this case UNESA uses Google LDAP. The attendance system by implementing WPA2 Enterprise has been tested by implementing the Technology Acceptance Model (TAM) method resulting in 43% answering strongly agree and 56% answering agreeing. The analysis is based on 78 employees who gave their assessments. Based on the results of the acceptance analysis of the system, it is stated that it can be applied at UNESA.

Keywords : Attendance; WIFI; WPA2; LDAP

Abstrak

Perkembangan teknologi memberikan efek positif bagi instansi maupun perusahaan, salahsatunya dengan adanya inovasi pendaftaran absensi karyawan menggunakan media jaringan internet. Model sistem absensi karyawan menggunakan jaringan internet tentu akan memudahkan dalam melakukan pengontrolan kehadiran karyawan. Jaringan internet merupakan bagian yang penting pada setiap instansi dalam membantu kinerjanya dan juga bisa digunakan sebagai sistem absensi. Penerapan WPA2 Enterprise digunakan sebagai autentifikasi menggunakan email dan password yang telah diberikan. Device yang telah terhubung dengan jaringan tersebut akan secara otomatis tercatat dalam sistem absensi karyawan. Penerapan WPA2 Enterprise membutuhkan bantuan freeradius dalam mengolah data autentikasi dari pegawai yang kemudian akan diverifikasikan lagi melalui LDAP, dalam hal ini UNESA menggunakan Google LDAP. Sistem absensi dengan menerapkan WPA2 Enterprise telah dilakukan pengujian dengan merapkan metode Technology Acceptance Model (TAM) menghasilkan 43% menjawab sangat setuju dan 56% menjawab setuju. Analisis tersebut berdasarkan 78 karyawan yang memberikan penilaiannya. Berdasarkan hasil analisis penerimaan terhadap sistem dinyatakan dapat diterapkan di UNESA.

Keywords : Absensi; WIFI; WPA2; LDAP

1. Pendahuluan

Perkembangan teknologi yang sangat cepat menjadi salah satu hal yang memberikan efek positif bagi instansi maupun perusahaan. Dengan adanya teknologi tersebut dapat membantu dalam pengololaan data informasi dengan jumlah besar dan data yang berkembang (Permadi, 2019). Pada kenyataannya kegunaan dari teknologi tentu beragam mulai dari pengelola dokumen, keamanan dokumen, pengiriman data, dan juga dalam melakukan proses absensi. Dalam tiap perusahaan pasti memiliki sebuah sistem absensi kehadiran karyawan. Dimana sistem absensi kehadiran ini juga sangat bergantung pada teknologi terkini untuk pengelolaan yang lebih cepat dan efisien untuk menunjang kinerja sumber daya manusia dan laju kembangnya instansi tersebut (Syarifudin, 2016). Kebanyakan sistem absensi pada instansi maupun perusahaan, masih banyak yang menggunakan sistem absensi dengan kartu rfid, ada juga menggunakan sidik jari, dan sampai dengan menggunakan pengenalan wajah (Permadi, 2018). Model absensi dari model kartu sampai dengan pengenalan wajah tersebut pasti melewati sebuah perkembangan terus menerus dengan tujuan akhir yakni memudahkan manusia dalam melakuakn

*) Penulis korespondensi: lanangprismana@unesa.ac.id

absensi. Sistem absensi tersebut terkadang dirasa kurang efektif karena keberadaan mesin absensi yang cukup jauh dari ruang kerja yang membuat para pekerja merasa terburu-buru untuk menuju ke tempat absensi sebelum menuju ke ruang kerjanya masing-masing sehingga kadang terjadi keterlambatan masuk ruang kerja (Sikumbang, 2020).

Untuk mengatasi kelemahan sistem absensi menggunakan biometri tersebut dibutuhkan pengembangan lanjut sistem absensi yang lebih fleksibel dan mudah tanpa perlu menuju ke tempat mesin absensi. Salah satu cara yang dapat mengatasi hal tersebut yakni dengan penerapam teknologi nirkabel dalam melakukan absensi. Peneraparan sistem absensi ini didukung dengan adanya jaringan wifi yang tersebar di titik tempat kerja dan setiap karyawan kebanyakan memiliki perangkat *smartphone*, maka kedua kebutuhan ini yang merupakan alat pendukung sistem absensi berbasis *wireless*. Cara kerja sistem absensi *wireless* ini dapat dibilang mudah yaitu setiap pegawai yang masuk wilayah kerja akan langsung terkoneksi dengan wifi dan secara otomatis mendeteksi keberadaan pegawai yang sudah terkoneksi dengan jaringan wifi tempat kerja. Dalam melakukan koneksi ke wifi karyawan diharuskan memasukan *username* dan *password* ke dalam jaringan wifi dan sekaligus mewakili absensi kehadiran melalui *login* ke jaringan wifi (Siregar, 2019).

Penelitian yang relevan tentang absensi kehadiran, menurut penelitian sebelumnya dengan judul "Aplikasi absensi menggunakan metode lock gps di PT. PLN (Persero) APP MALANG" dimana pada penelitian tersebut menunjukkan penggunaan sistem absensi berbasis gps, wifi dan aplikasi android berjalan dengan baik namun untuk mempersingkat langkah absensi dapat juga dilakukan hanya dengan authentikasi wifi yakni identitas login wifi sebagai parameter identitas pegawai dan *MAC address* dari wifi sebagai ganti lokasi dari karyawan (Akbar, 2015).

Berdasarkan uraian penelitan yang revelan diatas, maka peneliti untuk ingin menerapkan sistem absensi berbasis *WPA2-Enterprise*. Tujuan dari penelitian ini adalah membuat sistem absensi berbasis jaringan wifi internal instansi, melakukan proses pencatatan absensi masuk dan keluar berdasarkan aktivitas koneksi *wireless*, menganalisa tingkat kompatibilitas metode autentikasi berbasis *WPA2 Enterprise* (Bartoli, 2016).

2. Kerangka Teori

2.1. WPA2

WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA.

2.2. RADIUS

Radius (Remote Authentication Dial In User Service) merupakan sebuah protokal yang memiliki fungsi dalam hal manajemen autentifikasi, autorisasi, dan akuntansi (AAA) pada tiap komputer yang akan terhubung dan menggunakan jaringan internet, umumnya untuk jaringan wifi. RADIUS dikembangkan oleh Livingston Enterprises, pada tahun 1991 RADIUS ditetapkan sebagai standar protokol akses dan autentifikasi awal terlebih dahulu kemudian akhir (Haq, 2015).

Radius mengimplementasikan model AAA yang menggunakan elemen yang disebut dengan atribut untuk menggambarkan data mengenai autentikasi, autorisasi, dan akuntansi. Secara umum autentikasi digunakan untuk melakukan validasi identitas pengguna atau mesin yang akan dihubungi, autorisasi untuk memastikan alat pengguna untuk dicocokan dengan atribut yang diberikan seperti pada saat penggunaan VLAN ataupun pemberian limitasi (Wijaya, 2011).

Sedangkan untuk akuntasi digunakan untuk mencatat semua informasi dari hasil autorisasi dan informasi autentifikasi yang berhubungan dengan sesi aktif penggunaan. Atribut yang ada pada RADIUS umumnya digunakan untuk mengautentifikasi dan mengautorisasi pengguna untuk dilakukan penyaringan pembedaan akses yang diberikan untuk masing-masing pengguna dalam menggunakan jaringan yang kemudian akan dicatat kedalam log (Zuli, 2016).

Tabel 1 berikut ini merangkum secara umum atribut yang ada pada RADIUS beserta fungsinya:

Tabel 1. Atribut Radius

No	Atribut Radius	Deskripsi
1	User-Name	Nama pengguna
2	User-Password	Kata sandi pengguna
3	NAS-IP Address NAS-Port	Alamat IP Address dari NAS yang
4	Service Type	melakukan permintaan
5	Framed IP Address	Port dari NAS
6	Tunnel Type	Tipe layanan
7	Atribut Radius	IP yang didapatkan pengguna (dinamis)

2.3. Freeradius

Freeradius merupakan salah satu penyedia perangkat lunak *opensource* RADIUS yang penggunanya sangat banyak dan tersebar di dunia. Freeradius sangat berguna dan sangat menonjol untuk beberapa aspek yang meliputi kecepatan, skalabilitas pengguna, dan modul yang sangat lengkap dan memiliki banyak skema autentikasi

untuk dapat diterapkan di berbagai kondisi (Haq, 2015).

2.4. LDAP

LDAP merupakan standar protokol dasar yang mendukung mekanisme untuk mengakses direktori server dan berguna untuk melakukan autentikasi dan menyimpan informasi umum terkait *user* yang dapat digunakan untuk berbagai macam aplikasi. Informasi umum ini contohnya seperti nama, alamat, email, nomor induk pegawai, nomor telepon, maupun akun login dan data lainnya. LDAP juga memperbolehkan *client* untuk melakukan pencarian informasi dengan fitur filter dan akses kedalam informasi spesifik di direktori server (Darmadi, 2018).

LDAP secara umum akan terlihat memiliki fungsi seperti *database* secara umum yang gunanya untuk melakukan penyimpanan data. Tetapi berbeda dengan *database* relasional yang menggunakan tabel, kolom, dan relasi karena LDAP lebih seperti *database* dengan tipe NoSql walaupun direktori server jauh lebih dahulu ada. LDAP termasuk kedalam model *client-server*, dimana *client* akan mengirimkan *identifier* data ke server menggunakan protokol TCP/IP dan server akan mencari data pada DIT *(Directory Information Tree)* yang tersimpan di server. Jadi direktori server LDAP merupakan tipe *database* jaringan yang menyimpan informasi berhirarki seperti akar pohon (Ardian, 2012).

Menurut penjelasan yang ada pada *Basic Concepts website* LDAP, setiap entri LDAP adalah kumpulan informasi tentang sebuah entitas dimana setiap masukan terdiri dari 3 komponen utama yaitu *distuingished names (DNs)*, *attribute*, dan *object class*. Berikut ini merupakan penjabarannya (Muttaqin, 2016), yakni :

a. DNs

DNs yaitu *distuingished names* yang berarti nama tidak beraturan, yang memiliki arti yaitu identifikasi unik dalam hirarki *Directory Information Tree*. DN yang mempunyai lebih dari satu elemen maka dinamakan sebagai RDNs *(Rellative DNs)*. Misalnya, "uid = john.doe" mewakili RDN yang terdiri dari atribut dengan nama "uid" yang bernilai "john.doe". Jika RDN mempunyai beberapa pasangan nilai atribut, maka akan dipisahkan oleh tanda plus, seperti "givenName = John + sn = Doe". Nama akan dibedakan khusus terdiri dari nol RDNs (karena memiliki representasi string dimana nilai string kosong) kadang-kadang dikenal dengan "null DN" dan ada referensi jenis entri khusus yang dinamakan *DSE root* yang memiliki informasi terkait konten dan kemampuan server LDAP.

b. Attribute

Attribute yang berarti atribut, yakni memberikan dan menahan data sebuah masukan dimana tiap atribut tersebut memiliki tipe tersendiri. Tipe atribut merupakan skema elemen yang menspesifikasikan bagaimana atribut harus diperlakukan oleh client LDAP dan server. Semua atribut memiliki *identifier objek* (OID) dan akan memberikan nilai nol atau lebih nama atribut yang dapat digunakan untuk menunjuk atribut dari beberapa tipe.

c. Object Class

Object Class yang berarti kelas objek yang merupakan elemen skema untuk menentukan koleksi tipe atribut yang mungkin akan ada hubungannya dengan jenis objek tertentu, proses, ataupun entitas yang lain. Setiap masukan memiliki setidaknya sebuah struktur kelas objek yang mengindikasi macam-macam objek dari masukan *client*.

2.5. Google LDAP

Layanan *Secure LDAP* atau Google LDAP merupakan sebuah platform LDAP yang dimiliki google yang dapat menghubungkan banyak layanan berbasis *Cloud Identity* atau *G Suite*. Penggunaan Google *Secure LDAP* dapat digunakan sebagai server LDAP berbasis *cloud* untuk proses pencarian direktori, autentikasi, dan otorisasi (Aini, 2018).

Dengan adanya Google LDAP dapat memudahkan dalam memproses setiap pengecekan maupun pengelolaan autentikasi maupun otorisasi. Dimana dengan menggunakan Google LDAP dapat mengurangi proses dalam melakukan konfigurasi internal dan hanya perlu menghubungkan ke Google LDAP untuk ikut merasakan manfaat dari Google LDAP. Banyak aplikasi yang sudah didukung untuk dikolaborasikan dengan LDAP seperti Attlasian Jira, Gitlab, Freeradius, Open VPN, Sophos, dan lain sebagainya. Google LDPA juga sudah menyediakan cara untuk dapat terhubung dengan *Cloud LDAP* dengan panduan-panduan yang sudah tertera pada laman *G Suite*.

2.6. EAP

EAP merupakan protokol autentikasi yang didefinisikan dalam RFC3748 dimana memiliki kerangka kerja autentikasi yang dirancang untuk berjalan pada lapisan data link di mana konektivitas IP tidak tersedia. EAP dirancang untuk bekerja dengan koneksi *Point-toPoint*, dan kemudian diadaptasi untuk jaringan kabel IEEE 802 serta jaringan LAN nirkabel dan melalui Internet.

Arsitektur EAP melibatkan tiga komponen utama. Keterlibatan komponen-komponen ini dapat diilustrasikan dalam tumpukan protokol yang ditunjukkan pada Gambar 1. Ini memberikan kerangka dasar protokol permintaan / respons di mana berbagai metode EAP dapat diimplementasikan. Saat ini ada sekitar 40 metode berbeda yang didefinisikan. Beberapa metode autentikasi sudah ditentukan sebelumnya seperti LEAP, TLS, POTP, MD5, PSK, TTLS dan SIM.

Gambar 1. Skema EAP

Metode ini mendukung kredensial autentikasi yang mencakup tantangan, kata sandi, sertifikat, dan kunci. Metode lain dapat ditambahkan tanpa mengubah protokol jaringan atau mendefinisikan yang baru. Keuntungan utama arsitektur EAP adalah fleksibilitasnya untuk beradaptasi dengan berbagai metode autentikasi. Gambar 1 menunjukkan struktur dasar dari aliran pesan EAP. Metode ini mendukung kredensial autentikasi yang mencakup *challenge*, kata sandi, sertifikat, dan kunci. Metode lain dapat ditambahkan tanpa mengubah protokol jaringan atau mendefinisikan yang baru. Keuntungan utama arsitektur EAP adalah fleksibilitasnya untuk beradaptasi dengan berbagai metode autentikasi. Berikut beberapa metode autentikasi EAP :

a. PAP

PAP merupakan protokol autentikasi dimana pengguna mengirimkan kredensial ke server autentikasi yang tidak dienkripsi sebagai teks biasa. PAP juga salah satu protokol tertua untuk verifikasi paket, dimana PAP masih menggunakan proses jabat tangan dua arah.

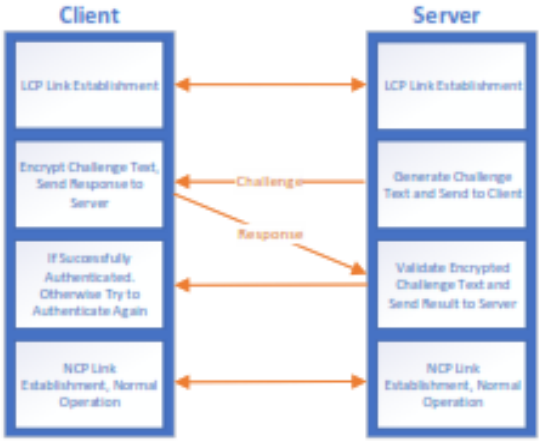
Verifikasi paket dimulai oleh pengguna yang mengirim paket dengan kredensial (nama pengguna dan kata sandi) di awal koneksi. PAP memiliki karakteristik dalam pengiriman kredensial ke server dalam teks biasa yang memberikan risiko besar terhadap akses yang tidak sah kepada pengguna yang dapat menangkap paket data menggunakan penganalisa protokol untuk mendapatkan kredensial. PAP rentan terhadap serangan seperti serangan *Eavesdropping* dan *Man-in-the-middle* (Yuliansyah, 2011).

Autentikasi kontrol akses jarak jauh juga dapat dilakukan menggunakan PAP, keuntungan tambahan dari PAP karena kompatibel dengan berbagai jenis server yang berjalan pada OS yang berbeda. Gambar 2 berikut ini memberikan aliran dasar model PAP.

b. MS-CHAP

MS-CHAP mengenkripsi informasi kata sandi sebelum mengirimkannya melalui jaringan PPP menggunakan metode enkripsi satu arah MD5. MS-CHAP tidak memerlukan *plaintext* atau kata sandi terenkripsiterbalik seperti yang dilakukan CHAP. Protokol MSCHAP tersedia dalam dua versi, MS-CHAPv1 (didefinisikan dalam RFC 2433) dan MS-CHAPv2 (didefinisikan dalam RFC 2759). MS-CHAPv2 mendukung autentikasi dua arah untuk memverifikasi identitas kedua sisi dari koneksi *point to point* dan menyediakan kunci kriptografi yang terpisah untuk data yang dikirim dan diterima berdasarkan kata sandi pengguna dan *string challenge* yang berubah-ubah. Dimana akan dirasa lebih aman daripada versi 1, karena pengguna yang sama akan memiliki kunci terpisah yang dihasilkan untuk setiap sesi. MS-CHAP mendukung *challenge peer* saat merespon dan merespon *authenticator* pada paket yang sukses untuk menghasilkan autentikasi bersama dikedua sisi.

Gambar 2. Skema PAP



Gambar 3. Skema MS-CHAP

c. EAP TLS

EAP-TLS (Transport Level Security) adalah metode EAP yang didasarkan pada RFC 2716 yang menggunakan *public key infrastructure* (PKI) dimana sertifikat digital untuk supplicant dan server autentikasi untuk memberikan autentikasi timbal balik antara *supplicant* dan server autentikasi. Sertifikat PKI akan berisi informasi tentang nama server atau informasi pengguna. Dalam hal ini akan memberikan sarana untuk autentikasi bersamaan antara klien dengan autentikator dan antara autentikator dengan klien. Secara dinamis proses ini menghasilkan dan mendistribusikan kunci enkripsi berbasis pengguna dan sesi untuk tujuan mengamankan koneksi. EAP-TLS dianggap sangat aman karena EAP-TLS menolak sebagian besar serangan, seperti serangan *replay* dan MITM. Fitur utama yang disediakan oleh EAP-TLS adalah penyambungan dan pertukaran kunci, autentikasi

bersama, dukungan untuk fragmentasi dan *reassembly*, dan fitur *fast reconnect*.

d. EAP-PEAP

EAP-PEAP mirip dengan TLS dimana menggunakan sertifikat *public key infrastructure* (PKI) untuk mengautentikasi. Tidak seperti TLS, EAP-PEAP membutuhkan satu sertifikat untuk mengautentikasi.

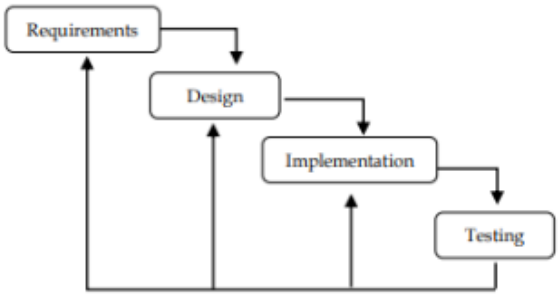
EAP PEAP termasuk metode autentikasi satu arah. Ada pengurangan dalam biaya dan kompleksitas pemrosesan dengan hanya mensyaratkan adanya sertifikat untuk diteruskan kepada autentikator, bukan pada klien. PEAP dapat berguna dalam enkripsi pesan, pertukaran kunci dan *fast reconnect*.

e. EAP-TTLS

EAP-TTLS dijelaskan dalam RFC 5281 yang merupakan lanjutan dari EAP-TLS yang menghilangkan sertifikat digital PKI dan mengurangi kompleksitas penerapan TLS. Proses autentikasi terjadi di dalam *secure tunnel* di mana perlindungan metode autentikasi akan dilakukan setelah validasi berhasil. Setelah verifikasi klien berhasil, makan jaringan *tunnel* akan dihancurkan. Kemudian pertukaran data terjadi menggunakan metode EAP yang kurang aman, seperti metode autentikasi MD5 atau metode yang sudah usang lainnya, seperti PAP atau CHAP.

3. Metode

Berikut ini merupakan alur jalannya penelitian untuk melakukan penelitian "sistem absensi berbasis *wireless* dengan wpa2 *enterprise*" secara umum digambarkan pada gambar 4, sebagai berikut:



Gambar 4. Alur Penelitian

Pada Gambar 4 membahas tentang alur penelitian penerapan sistem absensi berbasis *wireless* dengan wpa2 *enterprise*. Tahapan yang dilakukan pada penelitian ini yaitu analisis kebutuhan dengan melakukan studi pustaka untuk mencari literatur yang berkaitan untuk dapat dijadikan referensi pendukung dalam penelitian ini. Literatur yang digunakan berhubungan dengan *freeradius*, *eap* dan sistem absensi.

Kemudian membuat desain sistem autentikasi wifi yang berbasis wpa2 *enterprise* dengan dihubungan sistem LDAP sebagai sumber data. Pada tahap implementasi, penelitian ini menggunakan aplikasi *freeradius* dengan dihubungkan pada Google LDAP. Pada tahap pengujian sistem dilakukan untuk mengetahui kecocokan data absensi pegawai dari hasil autentikasi sistem wifi dengan keamanan WPA2 enterprise.

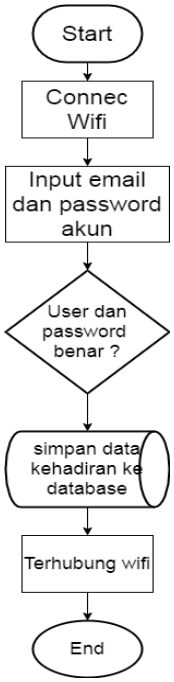
3.1. Pengumpulan data

Pada tahap ini penulis melakukan studi literatur terkait beberapa protokol keamanan untuk dipakai pada sistem autentikasi EAP atau WPA2 Enterprise. Diantara banyaknya protokol keamanan yang ada, penulis menekankan pada penerapan 2 protokol yang sudah banyak mendukung perangkat dan memiliki tingkah keamanan yang baik yakni EAP-TTLS dan EAP-PEAP.

Freeradius sendiri nantinya selain memiliki *database internal* juga akan dihubungkan ke sistem Google LDAP yang sudah dipakai oleh instansi Universitas Negeri Surabaya sebagai tempat percobaan dan pengambilan data dari penerapan sistem absensi berbasis *wpa2 enterprise* ini. Google LDAP membantu untuk mempersiapkan data berupa *email* dan *password* yang dimiliki tiap pegawai untuk masuk ke sistem SSO sebagai sumber data utama ketika proses autentikasi berlangsung.

3.2. Desain Sistem

Dalam sistem ini menggunakan PHP sebagai *user interface* untuk menampilkan data hasil absensi melalui jaringan *wpa2 enterprise*. Alur sistem dijelaskan pada Gambar 5 *flow chart* dibawah ini.



Gambar 5. Flowchart

Pada Gambar 5 menampilkan tentang alur desain sistem absensi berbasis *wireless* dengan *wpa2 enterprise* secara umum. Untuk memulai proses absensi dilakukan layaknya konek ke wifi pada umumnya namun pada tahap konek akan langsung diarahkan untuk melakukan autentikasi pada saat konek ke wifi dengan memasukkan username berupa *email* dan *password* untuk divalidasi ke Google LDAP, apabila sukses masuk maka juga sekaligus data kehadiran akan masuk ke dalam sistem.

3.3. Rancang Aplikasi

Penelitian ini mengimplementasikan sistem absensi berbasis wireless dengan wpa2 enterprise menggunakan freeradius dan Google LDAP sebagai system autentikasinya, dan untuk tampilan rekap absensi menggunakan bahasa pemrograman PHP dan database PostgreSQL untuk membuat sebuah website. Website digunakan untuk melihat data rekap absensi dari hasil autentikasi wifi sebagai sumber data kehadiran ketika pertama kali konek dan data pulang akan diambil dari waktu diskonek terakhir setiap harinya.

3.4. Ujicoba Produk

Ujicoba pada penelitian ini dilakukan oleh 10 pengguna layanan wifi internal kampus oleh pegawai Universitas Negeri Surabaya. 10 pengguna tersebut akan konek ke wifi kampus dan melakukan autentikasi agar bias terhubung ke jaringan internet sekaligus akan diambil data untuk sistem kehadiran datang dan pulang setiap harinya.

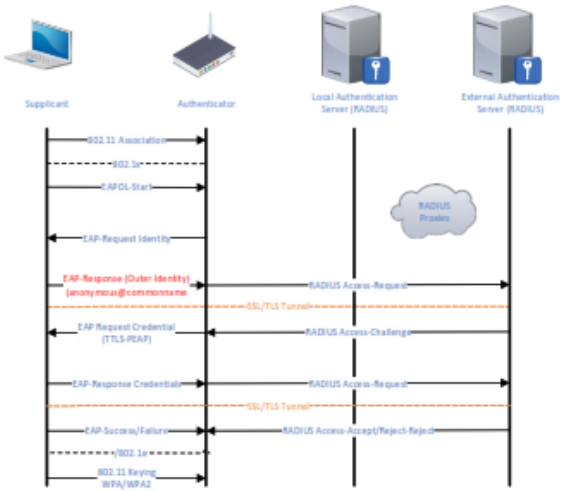
4. Hasil dan Pembahasan

Pengujian dilakukan dengan melalukan menghubungkan perangkat *smartphone* maupun laptop untuk tersambung ke jaringan wifi dengan memasukkan *email* dan *password* untuk dapat masuk ke jaringan wifi sekaligus untuk absensi kehadiran. Peran penting dari penerapan *WPA2 Enterprise* ini merupakan penentu keberhasilan dari sistem absensi. Jika sistem autentikasi *WPA2 Enterprise* berjalan dengan baik maka akan berimbas baik juga dalam penerapan sistem absensi oleh karena itu titik pemberatan pembahasan ada pada 2 pembahasan yakni *WPA2 Enterprise* sendiri dengan system absensi yang bersumber data dari transaksi data *WPA2 Enterprise.*

4.1. Flowchart WPA2 Enterprise

Dibawah ini merupakan alur pemrosesan EAP *WPA2 Enterprise* dalam memproses tiap *request* autentikasi oleh pengguna yang juga dijelaskan pada Gambar 6.

1) Assosiation
   Pada tahap Assosiation ini, *supplicant / client* melakukan asosiasi ke SSID yang dituju untuk disambungkan ke *Access Point*.



Gambar 6. Alur pemrosesan EAP (WPA2 Enterprise)

2) EAP Initialization
   Pada tahap ini, supplicant / client melakukan *request identity* kepada *Authenticator (Access Point)* untuk mengirimkan EAPOL awal untuk memulai inisialisasi koneksi EAP ke *Access Point*. Selanjutnya *Access Point* akan mengirimkan ulang respon *request identity* kepada *client* untuk ditanyai mengenai identitas awal *client* sebelum autentikasi selanjutnya.
3) EAP Response dan Access Request
   Pada tahap ini *client* mengirimkan identitas awal sebagai *anonymous user* dan melakukan akses *request* kepada *Radius Server (Internal Radius)* dan *External Radius* (Google LDAP). *Anonymous* user akan selalu dipakai sebagai identitas awal saat pertama kali EAP proses dimulai oleh *supplicant*, dikarenakan supplicant belum diminta untuk memasukkan akun kredensial secara langsung sebelum proses challenge dimulai, dimana *access challenge* akan diminta setelah tahap *request* ini.
4) EAP Access Challenge and Credentials
   Pada tahap ini data *access request* akan dikembalikan lagi kepada *access point* untuk diteruskan dan diminta *access challenge* kepada *supplicant / client. Access challenge* yang diminta berupa protokol EAP apa yang digunakan, *username* dan *password* apa yang akan dikirimkan sebagai identitas untuk diproses autentikasinya. Tahap ini diharuskan *supplicant / client* untuk memasukkan *username* dan *password* untuk dapat diteruskan dan ditentukan boleh atau tidaknya ke proses selanjutnya.
5) EAP Decision
   Pada tahap ini data inputan username dan *password* oleh *supplicant* akan diteruskan ke *authentication server (Internal Radius)* untuk diverifikasi apakah ada data yang sesuai dengan yang direspon oleh *autenticator*. Jika data sesuai maka akan ditentukan status EAPnya sukses dan jika data tidak sesuai maka akan diteruskan

pengecekan ke External Radius dalam hal ini menggunakan data sumber Google LDAP. Jika *response* dari *supplicant* yang berupa *username* dan *password* cocok / ada dalam database maka akan ditentukan status EAPnya success, dan jika tidak maka status EAPnya *failed* dan ditolak untuk masuk kedalam jaringan.

Untuk yang status EAP sukses maka akan diberikan umpan balik *response* berupa *attribute* yang sebeldumnya sudah ditentukan bisa berupa limitasi, *vlan attribute* maupun *attribute* yang lain yang dapat disertakan untuk diberikan kepada *supplicant*.

4.2. Implementasi Sistem

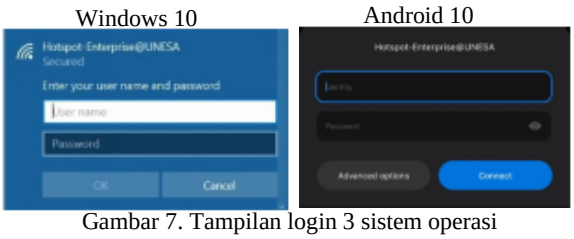
Pada penelitian ini menggunakan protokol enkripsi PEAP dan TTLS untuk penerapan *WPA2 Enterprise*, dan menggunakan *external radius* dalam hal ini menggunakan Google LDAP karena instansi Universitas Negeri Surabaya menggunakan akun SSO dari layanan *google education* sebagai one gate sistem. Jadi untuk tetap menerapkan *single account* untuk semua akses digunakan pula akun email instansi berdomain unesa.ac.id untuk autentikasi jaringan wifi yang sekaligus untuk absensi kehadiran pegawai. Berdasarkan data yang diambil pada tanggal 1 Mei hingga 30 Juni 2020. Tercatat data yang berhasil masuk sebagai data autentikasi sekaligus absensi oleh pegawai UNESA ada sebanyak 20 orang yang sudah mencoba menggunakan jaringan *WPA2 Enterprise*. Dan dari data tersebut terdapat data yang berhasil dan gagal.

Berikut Tabel 2 berdasarkan sistem operasi yang sukses dan gagal berdasarkan hasil implementasi.

Tabel 2. Percobaan tipe EAP

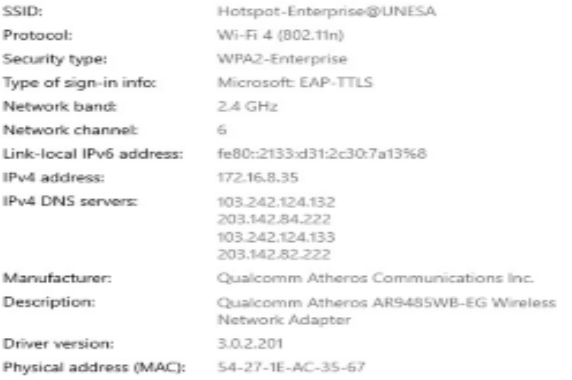
Sistem Operasi	EAP Type	Status
Windows 7	PEAP	Gagal
Windows 7	TTLS	Gagal
Windows 8/8.1	PEAP	Gagal
Windows 8/8.1	TTLS	Sukses
Windows 10	PEAP	Gagal
Windows 10	TTLS	Sukses
Mac OS	PEAP	Sukses
Mac OS	TTLS	Sukses
Ubuntu 18/20	PEAP	Sukses
Ubuntu 18/20	TTLS	Sukses
Android 5.1 Lolipop	PEAP	Sukses
Android 5.1 Lolipop	TTLS	Sukses
Android 7 Nougat	PEAP	Sukses
Android 7 Nougat	TTLS	Sukses
Android 8 Oreo	PEAP	Sukses
Android 8 Oreo	TTLS	Sukses
Android 9 Pie	PEAP	Sukses
Android 9 Pie	TTLS	Sukses
Android 10Queen Cake	PEAP	Sukses
Android 10Queen Cake	TTLS	Sukses

Berikut tampilan dari *login WPA2 Enterprise* dari tiga sistem operasi berbeda disajikan pada Gambar 7.



Gambar 7. Tampilan login 3 sistem operasi

Pada Gambar 7 diperlukan mengisi *username* dan *password* terlebih dahulu, pastikan dalam memasukan *username* dan *password* sudah benar. Jika benar maka akan masuk ke tampilan berhasil *login* seperti Gambar 8 berikut.



Gambar 8. Halaman login

4.3. Pengujian Sistem

Pengujian sistem dilakukan oleh 78 pengguna wifi di UNESA oleh pegawai yang akan melakukan koneksi ke jaringan wifi kampus dengan maksud agar bisa mengerjakan tugas-tugasnya yang kebanyakan membutuhkan koneksi internet dan sekaligus untuk data absensi kehadiran.

MAC Address	IP Address	MCS	RSSI	TxRate (kbps)	RxRate (kbps)	STA Mode
18:3a:2d:08:ff:6b	192.168.1.5	7	-58	65000	65000	11n
c0:bd:d1:22:73:6b	192.168.1.2	12	-80	78000	39000	11n
ec:51:bc:67:8c:f7	192.168.1.3	7	-72	65000	1000	11n
e8:39:df:05:e4:c3	192.168.1.6	7	-63	65000	65000	11n
64:5a:04:b7:f2:88	192.168.1.9	5	-74	52000	65000	11n
d0:9c:7a:1c:06:4c	192.168.1.7	7	-72	65000	65000	11n

Gambar 9. Tampilan login berhasil dan masuk

Pada Gambar 9 terlihat seteleh proses login berhasil, pada *website* rekap akan langsung terlihat data waktu mulainya sebagai data absensi masuk, dan waktu berakhir masing kosong karena status wifi masih terkoneksi.

MAC Address	IP Address	MCS	RSSI	TxRate (kbps)	RxRate (kbps)	STA Mode
18:3a:2d:08:ff:6b	192.168.1.5	7	-58	65000	65000	11n
c0:bd:d1:22:73:6b	192.168.1.2	12	-80	78000	39000	11n
ec:51:bc:67:8c:f7	192.168.1.3	7	-72	65000	1000	11n

Gambar 10. Tampilan disconnect dan tercatat sebagai absensi keluar

Pada Gambar 10 terlihat sesaat setelah melalui diskonek dari jaringan wifi maka akan langsung tercatat waktu berakhir sebagai absensi keluar.

5. Kesimpulan

Dari hasil ujicoba dapat diambil kesimpulan bahwa dengan menerapkan sistem autentikasi WPA2 Enterprise dapat dimanfaatkan pula untuk sistem absensi pada saat melakukan koneksi ke jaringan wifi sebagai data absensi masuk dan pada saat terputus dari jaringan wifi sebagai data absensi keluar. Rekap hasil absensi perhari akan diambil dari banyaknya data kemudian disortir berdasarkan data paling awal untuk data kehadiran masuk dan paling akhir untuk data kehadiran keluar .

Tingkat fleksibilitas *WPA2 Enterprise* cukup baik karena dapat menyimpan akun yang sudah pernah digunakan dan berhasil masuk ke jaringan jadi ketika koneksi pertama berhasil maka untuk selanjutnya tidak akan ditanya *username* dan *password* lagi, fitur *session resumption* dapat langsung berjalan dengan baik dalam hasil penelitian ini untuk kedua tipe EAP.

Dan tipe eap yang cocok untuk penerapan *WPA2 Enterprise* berdasarkan penelitian ini adalah memakai tipe TTLS karena lebih banyak didukung oleh banyak sistem operasi dan berdasarkan hasil pengujian *WPA2 Enterprise* lebih banyak didukung oleh sistem operasi android jadi untuk sistem absensi lebih baik menggunakan *smartphone* untuk dijadikan penentu pengambilan data absensi dari aktivitas koneksi wifi.

Daftar Pustaka

Akbar, R.M., Nanu, P., 2015. Aplikasi Absensi Menggunakan Metode Lock GPS dengan Android Di Pt. Pln (Persero) App Malang Basecamp Mojokerto. Majapahit Techno, 55-63.

Ardian, Y., 2012. Implementasi sistem otentikasi pada pengguna jaringan hotspot di Universitas Kanjuruhan Malang guna meningkatkan keamanan jaringan. Jurnal Informatika, 34-41.

Aini, Q., Rahardja, U., Naufal, R.S., 2018. Penerapan Single Sign On Dengan Google Pada Website Berbasis Yii Framework. Sisfotenika 8 (1).

Bartoli, A., Medvet, E., Onesti, F., 2018. Evil Twins and WPA2 Enterprise: A Coming Secutity Disaster? Computers & Security 74 Elsevier.

Darmadi, E.A., 2018. Perancangan sistem otentikasi radius pada pengguna jaringan wireless untuk meningkatkan keamanan jaringan komputer. Jurnal Ikra-Ith Informatika 2 (3).

Permadi, G.S., Vitadiar, T.Z., Kistofer, T., 2019. Sistem evaluasi bahan pembelajaran menggunakan metode Dematel dan ANP, J. Sist. Inf. Bisnis 9(2), 228-235.

Permadi, G.S., Adi, K.R., Gernowo, 2018. Application Mail Tracking Using RSA Algorithm As Security Data and Hot-Fit A Model For Evaluation System, In E3s Web Of Conferences.

Haq, M.Z.U., Timur, T.W., Rahmadi, Y., 2015. Implementasi AAA menggunakan radius sever pada jaringan VPN (study kasus : PT. Forum Agro Sukses Timur). Undergraduate Thesis, Universitas Muhammadiyah Jember.

Muttaqin, A.H., Rochim, A.F., Widianto, E.D., 2016. Sistem autentikasi hotspot menggunakan ldap dan radius pada jaringan internet wireless prodi teknik sistem komputer. Jurnal Teknologi dan Sistem Komputer 4 (2).

Syarifudin, S. & Rahadjo, B., 2016. Perbandingan Teknologi Wireless Untuk Sistem Absensi Pada Smart University. Senter, 37-45.

Sikumbang, M.A., Habibi, R., & Pane, S.F., 2020. Sistem informasi absensi pegawai menggunakan metode RAD dan metode LBS pada koordinat absensi. Jurnal Media Informatika Budidarma, 59-64.

Siregar, R.L., 2019. Implementasi Jaringan Hotspot Dengan Captive Portal Zeroshell Dan User Management Ldap. 87-96.

Wijaya, B., 2011. Membangun server AAA menggunakan protokol remote access dial in user service. Diploma Polteknik Negeri Jember, Jember.

Yuliansayh, H., 2011. Optimalisasi radius server sebagai system otentikasi dan otorisasi untuk proses login multi aplikasi web berbasis PHP. Skripsi Universitas Ahmad Dahlan, Yogyakarta.

Zuli, F., 2016. Penerapan metode simple queue untuk manajemen bandwidth dengan router mikrotik. Jurnal Satya Informatika, 2333.