Penerapan Sistem Absensi Kehadiran Pegawai Berbasis Jaringan Wireless WPA2 Enterprise

Wahyu Khamdani[1], IGL. Putra Eka Prismana[2], Aditya Prapanca[3], Dodik Arwin Dermawan[4]

[1,2,3,4] Teknik Informatika, Universitas Negeri Surabaya

[1]wahyu@mhs.unesa.ac.id
[2]lanangprismana@unesa.ac.id
[3]adityaprapanca@unesa.ac.id
[4]dodikdermawan@unesa.ac.id

***Abstrak*—Sistem absensi kehadiran dan jaringan internet merupakan dua hal yang berkaitan dengan teknologi yang umumnya pasti dibutuhkan pada tiap perusahan ataupun instansi. Umumnya pegawai setiap datang dan pulang diharuskan untuk melakukan absensi dengan datang ke mesin absensi dan melakukan absensi baik melalui *fingerprint* atau deteksi wajah, dimana proses itu terkadang memakan waktu untuk dapat masuk ke ruang kerja karena ruang kerja dan lokasi mesin absensi yang cukup jauh. Untuk membantu pegawai dalam melakukan 2 hal sekaligus yakni autentikasi wifi dan melakukan absensi kehadiran diperlukan sistem absensi dengan menggunakan jaringan wifi. Untuk menerapkan sistem autentikasi jaringan wifi yang cocok untuk kehadiran dibutuhkan sistem autentikasi yang langsung dapat menggunakan *username* dan *password* tanpa *captive portal* yang membutuhkan bantuan *browser* untuk autentikasi. Maka untuk memenuhi kebutuhan itu dapat terselesaikan dengan memakai metode autentikasi WPA2 *Enterprise*, dimana tiap pegawai hanya perlu memasukkan *username* dan *password* berupa email dan *password* yang diberikan instansi / pegawai, maka akan langsung berhasil masuk ke jaringan wifi dan sekaligus terekam untuk melakukan absensi kehadiran. Untuk menerapkan WPA2 *Enterprise* ini dibutuhkan bantuan *freeradius* dalam mengolah data autentikasi dari pegawai yang kemudian akan diverifikasikan lagi melalui LDAP, dalam hal ini UNESA menggunakan Google LDAP. Alur dari autentikasinya yakni pegawai melakukan koneksi ke jaringan wifi kemudian memasukkan *username* dan *password*, kemudian *access point* akan meneruskan proses verifikasi ke *freeradius* dan *freeradius* akan membantu melakukan verifikasi dan validasi akun. Data hasil absensi diambil dari aktivitas berhasil login dari autentikasi wifi dimana dapat paling awal dan akhir akan dipakai datanya untuk data kehadiran.**

Kata Kunci—**sistem absensi, wpa2 enterprise, freeradius.**

I. PENDAHULUAN

Perkembangan teknologi yang sangat cepat menjadi salah satu hal yang berguna bagi instansi maupun perusahaan. Dengan adanya teknologi akan sangat membantu instansi dalam mengelola informasi dalam jumlah besar dan data yang berkembang.

Dalam perkembangannya, tiap perusahaan pasti memiliki sebuah sistem absensi kehadiran pegawai. 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. Umumnya instansi maupun perusahaan, masih banyak yang menggunakan sistem absensi dengan sistem *biometric*, dimana 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.

Untuk mengatasi hal tersebut dibutuhkan sistem absensi yang lebih fleksibel dan mudah tanpa perlu menuju ke tempat mesin absensi berada. Salah satu yang dapat mengatasi hal tersebut yakni dengan sistem absensi berbasis jaringan *wireless*. Dimana dengan adanya jaringan *wifi* yang tersebar di wilayah kerja dan hampir setiap tempat dapat terjangkau jaringan *wifi*, serta tiap pegawai kebanyakan pasti memiliki perangkat *smartphone*, maka sistem absensi yang efektif yakni absensi berbasis *wireless* dimana setiap pegawai yang masuk wilayah kerja akan langsung terkoneksi dan secara otomatis mendeteksi keberadaan pegawai yang sudah terkoneksi dengan jaringan wifi tempat kerja yang telah melakukan autentikasi berupa *username* dan *password* ke dalam jaringan wifi dan dapat mewakili absensi kehadiran melalui login ke jaringan wifi.

Untuk memperlancar sistem absensi berdasarkan *wireless* agar secara otomatis masuk ke jaringan wireless tanpa proses *login* ke sistem *captive portal*, maka diperlukan metode autentikasi berbeda yakni dengan menggunakan metode autentikasi berbasis *WPA2-Enterprise*.

Dengan metode *WPA2-Enterprise* maka pegawai yang akan masuk ke jaringan *wireless* dapat langsung terkoneksi dengan *username email* beserta *password* yang dimiliki untuk diteruskan proses autentikasinya pada setelan koneksi *wireless*. Proses untuk memasukkan *username* dan *password* hanya membutuhkan satu kali setelan, dan untuk selanjutkan tidak perlu lagi memasukkan *username* dan *password* karena sudah masuk ke setelan *wireless* pada tiap perangkat.

Penelitian yang relevan tentang absensi kehadiran, menurut penelitian Ronny (2017) dengan judul "A*plikasi 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 pegawai.

Berdasarkan uraian penelitan yang revelan diatas, maka peneliti untuk ingin menerapkan sistem absensi berbasis *WPA2-Enterprise.* Tujuan dari penelitian ini adalah: (1) Membuat sistem absensi berbasis jaringan wifi internal instansi, (2) Melakukan proses pencatatan absensi masuk dan keluar berdasarkan aktivitas koneksi wireless, (3) Menganalisa

tingkat kompatibilitas metode autentikasi berbasis WPA2-*Enterprise*.

II. TINJAUAN PUSTAKA

A. 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.

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. 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 menautentifikasi dan mengautorisasi pengguna untuk dilakukan penyaringan pembedaan akses yang diberikan untuk masing-masing pengguna dalam menggunakan jaringan yang kemudian akan dicatat kedalam log.

Tabel 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*	Alamat IP *Address* dari NAS yang melakukan permintaan
4	*NAS-Port*	Port dari NAS
5	*Service Type*	Tipe layanan
6	*Framed IP Address*	IP yang didapatkan pengguna (dinamis)
7	*Tunnel Type*	Tipe tunnel atribut yang dilekatkan ke pengguna

B. 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.

C. 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*.

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.

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:

1. 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.

2. *Attribute*

   Attribute yang berarti atribut, yakni memberikan dan menahan data sebuah masukan dimana tiap atribut 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.

3. *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*.

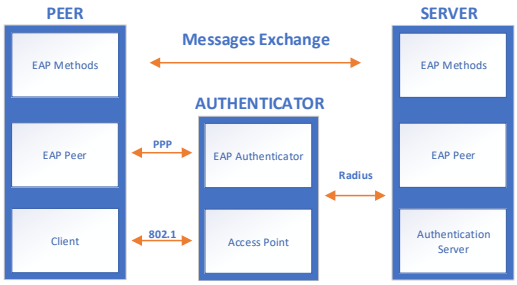
D. Google LDAP

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. 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*.

E. 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-to-Point*, 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.



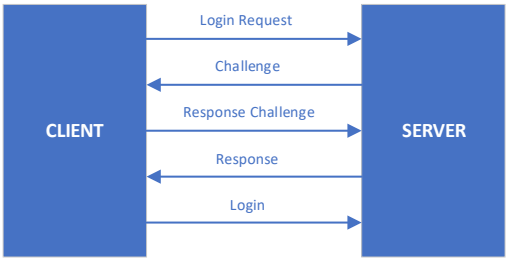
Gambar 1. Skema EAP

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 :

1. 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*. 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.

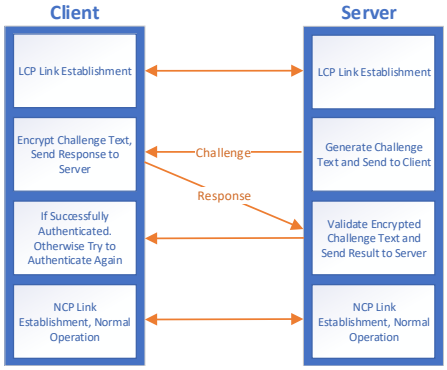


Gambar 2. Skema PAP

2. 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 terenkripsi terbalik seperti yang dilakukan CHAP. Protokol MS-CHAP 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 3. Skema MS-CHAP

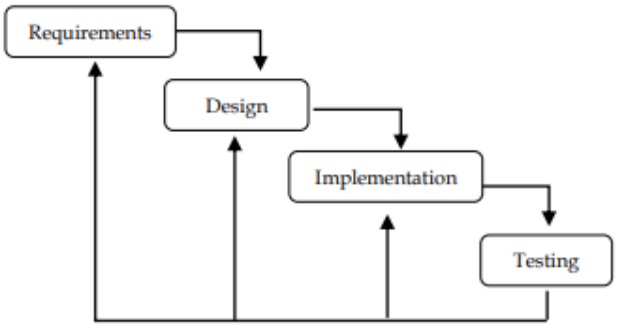
3. EAP TLS
   EAP-TLS (*Transport Level Security*) adalah metode EAP yang didasarkan pada RFC 2716 yang menggunakan *public key infrastructure* (PKI) dimana sertifikat digital untuk *supplicant* dan *server* autentikasi untuk memberikan autentikasi timbal balik antara supplicant dan *server* autentikasi. 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*.

4. 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*.

5. 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. EAP-TTLS memperbolehkan penggunaan protokol berbasis *password* lama atau usang terhadap autentikasi yang ada pada *database* ketika melindungi keamanan dari protokol yang sudah lama melawan adanya serangan *man in the middle* dan serangan eavesdropping.

III. METODOLOGI PENELITIAN

Berikut ini merupakan alur jalannya penelitian untuk melakukan penelitian "sistem absensi berbasis *wireless* dengan wpa2 *enterprise*" secara umum digambarkan pada gambar 1, sebagai berikut:



Gambar 4. Alur Penelitian

Gambar 1 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*.

A. Pengumpulan data

Pada tahap ini penulis melakukan studi literatur terkait beberapa protokol keamanan untuk dipakai pada sistem autentikasi EAP atau WPA2 *Enterprise*. Diantara

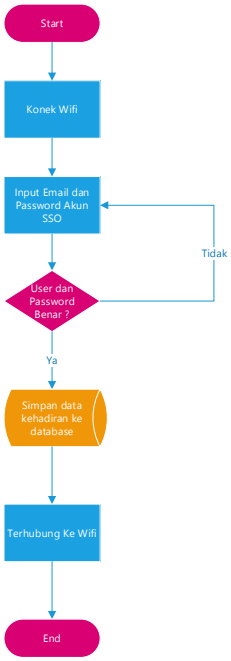
banyaknya protokol keamanan yang ada, penulis menekankan pada penerapan 2 protokol yang sudah banyak mendukung perangkat dan memiliki tingkah keamanan yang baik yakni EAP-TTLS dan EAP-PEAP.

Dalam penelitian ini, penulis menggunakan aplikasi freeradius sebagai inti dari penerapan sistem autentikasi yang nantinya akan dipakai sebagai titik pengambilan data untuk pemrosesan absensi kehadiran. Freeradius nantinya akan digunakan untuk mengaktifkan sistem autentikasi yang nantinya dipakai oleh *access point* sebagai autentikator menuju ke freeradius untuk diproses verifikasi data autentikasinya.

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.

B. 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* sebagai berikut :



Gambar 5. Alur Desain sistem

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.

C. Rancang aplikasi

Penelitian ini mengimplementasikan sistem absensi berbasis *wireless* dengan wpa2 *enterprise* menggunakan freeradius dan Google LDAP sebagai sistem 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.

D. 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 bisa terhubung ke jaringan internet sekaligus akan diambil data untuk sistem kehadiran datang dan pulang setiap harinya.

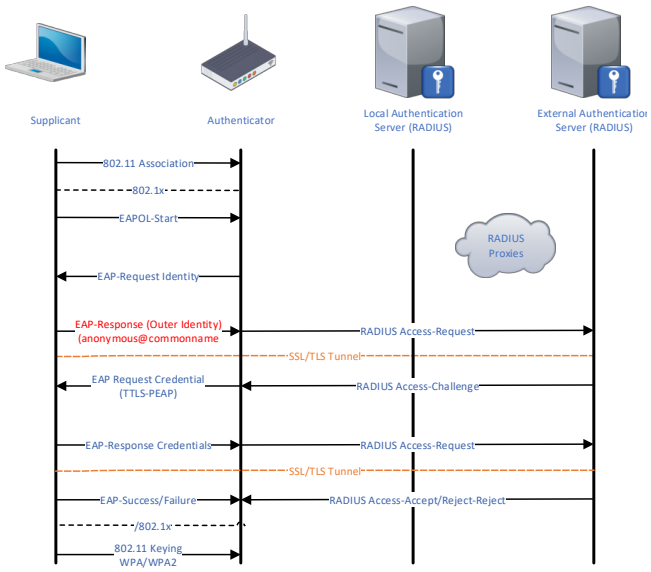
IV. HASIL DAN PEMBAHASAN

Bab ini membahas tentang penelitian dan pengujian terhadap impelentasi yang dilakukan serta analisis kompatibilitas dari protokol keamanan WPA2 *Enterprise* yang digunakan untuk dimanfaatkan sebagai sumber data absensi kehadiran. 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 sistem absensi yang bersumber data dari transaksi data WPA2 *Enterprise*.

A. *Flowchart*

1. *WPA2 Enterprise Flowchart*

Dibawah ini merupakan alur pemrosesan EAP WPA2 *Enterprise* dalam memproses tiap *request* autentikasi oleh pengguna.



Gambar 6. Alur pemrosesan EAP (WPA2 *Enterprise*)

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

b. 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.

c. 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.

d. 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.

e. 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 sebelumnya sudah ditentukan bisa berupa limitasi, vlan *attribute* maupun *attribute* yang lain yang dapat disertakan untuk diberikan kepada *supplicant*.

B. *Flowchart* rekap absensi
Dibawah ini merupakan alur untuk mengakses rekap hasil absensi dari autentikasi WPA2 *Enterprise.*

1. Akses *website* rekap
Untuk mengakses hasil rekap dari absensi perlu masuk dahulu kedalam *website* yang beralamatkan https://absensiwireless.unesa.ac.id.

2. Masuk dengan akun email berdomain @unesa.ac.id
Untuk dapat masuk kedalam *website* rekap harus masuk dengan menggunakan akun *email* unesa sebagai identitas yang sama dengan yang digunakan untuk masuk ke sistem autentikasi wifi berbasis WPA2 *Enterprise*.

3. Setelah berhasil masuk kedalam *website* absensi, rekap bisa langsung dicek pada menu “Rekap Absen” secara *realtime*.

C. Implementasi *Database*

Tabel 2. Tabel *users*

users		
name	**type**	**length**
id	int4	32
name	varchar	255
email	varchar	255
password	varchar	60
provider	varchar	255

provider_id	varchar	255
remember_token	varchar	255
questionmark	varchar	100
created_at	timestamp	6
updated_at	timestamp	6

tabel 3. tabel radacct

radacct		
name	**type**	**length**
radacctid	int8	64
acctsessionid	text	0
acctuniqueid	text	0
username	text	0
realm	text	0
nasipaddress	inet	0
nasportid	text	0
nasporttype	text	0
acctstarttime	timestamptz	6
acctupdatetime	timestamptz	6
acctstoptime	timestamptz	6
acctinterval	int8	64
acctsessiontime	int8	64
acctauthentic	text	0
connectinfo_start	text	0
connectinfo_stop	text	0
acctinputoctets	int8	64
acctoutputoctets	int8	64
calledstationid	text	0
callingstationid	text	0
acctterminatecause	text	0
servicetype	text	0
framedprotocol	text	0
framedipaddress	inet	0

D. Implementasi Sistem

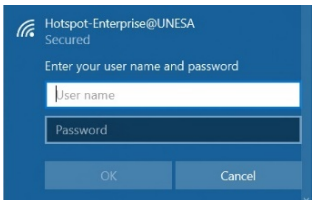
Pada penelitian ini menggunakan protokol enkripsi PEAP dan TTLS untuk penerapan WPA2 *Enterprise*, dan menggunakan *external* radius dalam hal ini menggunakan Google LDAP karena instansi Universitas Negeri Surabaya menggunakan akun SSO dari layanan google *education* sebagai *one gate* sistem. Jadi untuk 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 10 orang yang sudah mencoba menggunakan jaringan WPA2 *Enterprise*. Dan dari data tersebut terdapat data yang berhasil dan gagal. Berikut tabel berdasarkan sistem operasi yang sukses dan gagal berdasarkan hasil implementasi.

tabel 4. Tabel hasil percobaan tipe EAP berdasarkan jenis sistem operasi

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 Lollipop	PEAP	Sukess
Android 5.1 Lollipop	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 10 Queen Cake	PEAP	Sukses
Android 10 Queen Cake	TTLS	Sukses

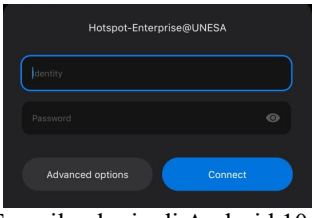
Berikut ini adalah tampilan dari login WPA2 *Enterprise* dari berbagai sistem operasi:

1. Windows 10



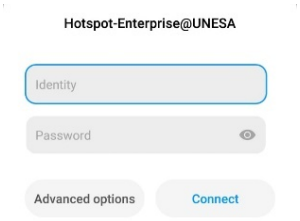
Gambar 7. Tampilan login di Windows 10

2. Android 10



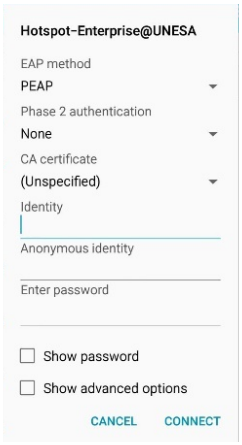
Gambar 8. Tampilan login di Android 10

3. Android 7



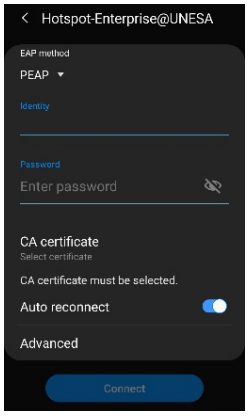
Gambar 9. Tampilan login di Android 7

4. Android 5.1



Gambar 10. Tampilan login di Android 5.1

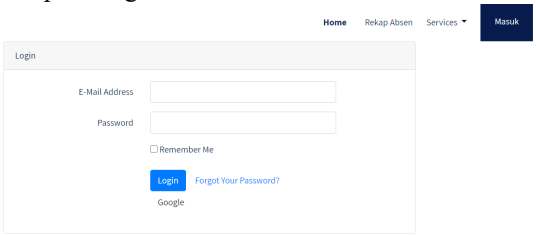
5. Android 9



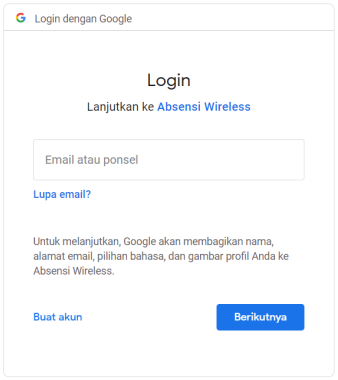
Gambar 11. Tampilan login di Android 9

Dan berikut ini merupakan tampilan dari *website* rekap absensi :

1. Tampilan login awal

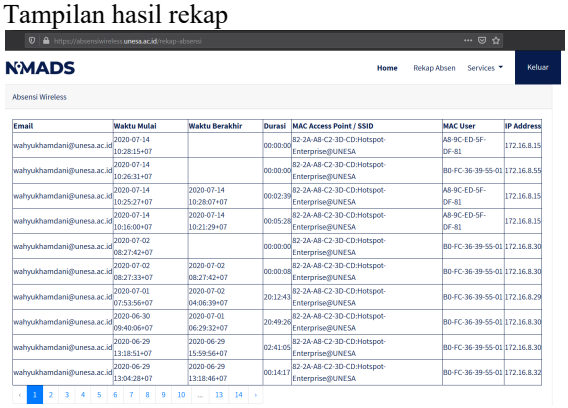


Gambar 12. Tampilan *login website* rekap



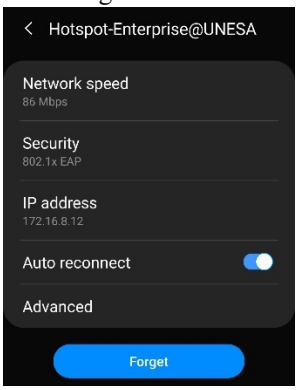
Gambar 13. Tampilan login rekap melalui *social login* google

2. Tampilan hasil rekap



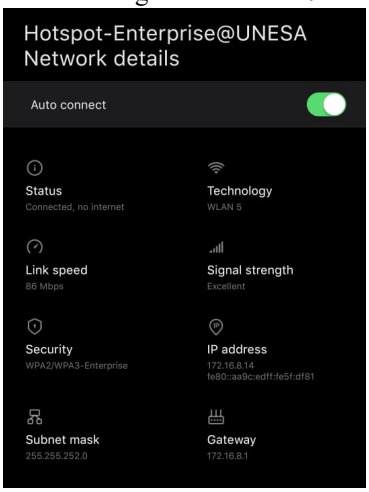
Gambar 14. Tampilan hasil rekap absen

3. Tampilan berhasil login di Android 9



Gambar 15. Tampilan berhasil login di Android 9

4. Tampilan berhasil login di android 10



Gambar 16. Tampilan berhasil *login* di Android 10

5. Tampilan berhasil *login* di Windows 10

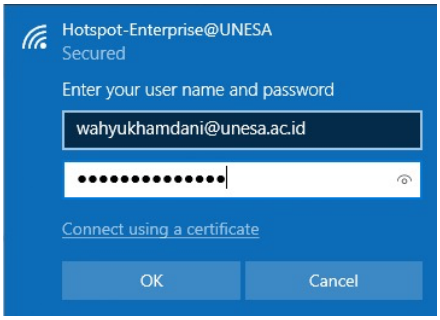
SSID:	Hotspot-Enterprise@UNESA
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Enterprise
Type of sign-in info:	Microsoft: EAP-TTLS
Network band:	2.4 GHz
Network channel:	6
Link-local IPv6 address:	fe80::2133:d31:2c30:7a13%8
IPv4 address:	172.16.8.35
IPv4 DNS servers:	103.242.124.132 203.142.84.222 103.242.124.133 203.142.82.222
Manufacturer:	Qualcomm Atheros Communications Inc.
Description:	Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Driver version:	3.0.2.201
Physical address (MAC):	54-27-1E-AC-35-67

Gambar 17. Tampilan berhasil login di Windows 10

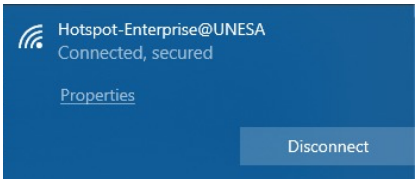
E. Pengujian Sistem

Pengujian sistem dilakukan oleh 10 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.

Dibawah ini merupakan contoh *login* wifi yang dilakukan oleh pegawai dengan menggunakan Windows 10.



Gambar 18. Pengujian login di Windows 10



Gambar 19. Tampilan berhasil terkoneksi wifi login windows 10

Gambar 20. Tampilan rekap hasil absensi masuk

Pada gambar 20 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.

Gambar 21. Tampilan rekap hasil absensi keluar

Pada gambar 21 terlihat sesaat setelah melalui diskonek dari jaringan wifi maka akan langsung tercatat waktu berakhir sebagai absensi keluar.

V. KESIMPULAN & SARAN

A. Kesimpulan

Pengujian dilakukan dengan melakukan *login* wifi dengan akun email milik masing-masing pegawai. Pada saat *login* wifi akan ditanyakan *username* dan *password* kemudian untuk beberapa sistem operasi android akan ditanyakan tentang tipe eap yang digunakan, dan dalam pengujian ini memakai eap ttls dan peap untuk dibandingkan kompatibilitasnya. 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.

B. Saran

Untuk penelitian selanjutnya dapat ditambahkan aplikasi android untuk konfigurasi *username* dan *password* agar saat melakukan koneksi ke SSID wifi yang sudah ditentukan bisa langsung terkoneksi tanpa ditanya *username* dan *password*.

REFERENSI

[1] Abo-Soliman, M. A., & Azer, M. A. (2018). Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments. *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 268-273). Prague, Czech Republic: IEEE.

[2] Adikara, F. (2015). PEMANFAATAN MAC ADDRESS HOSTSPOT DALAM PENGEMBANGAN SISTEM ABSENSI GPS DALAM RANGKA MENINGKATKAN KEAKURATAN POSISI PENGGUNA. *Jurnal Sistem Informasi*, 454-461.

[3] 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.

[4] Bartoli, A., Medvet, E., & Onesti, F. (2018). Evil twins and WPA2 Enterprise: A coming secutity disaster? *Computers & Security 74 Elsevier*.

[5] Chifor, B.-C., Teican, S., Togan, M., & Gugulea, G. (2018). A Flexible Authorization Mechanism for Enterprise Networks Using Smart-Phone Devices. *2018 International Conference on Communications (COMM)* (pp. 437-440). Bucharest, Romania: IEEE.

[6] Chughtai, F., UlAmin, R., Malik, A. S., & Saeed, N. (2019). Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP. *The International Arab Journal of Information Technolog*, 862-870.

[7] Chughtai, F., UlAmin, R., Sattar Malik, A., & Saeed, N. (2019). Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP. *The International Arab Journal of Information Technology*, 862-870.

[8] Cristescu, G.-C., Croitoru, V., & Sorici, V. (2016). Implementing an AAA-RADIUS solution based on EAP. *2016 12th IEEE International Symposium on Electronics and Telecommunications (ISETC).* IEEE: Timisoara, Romania.

[9] Duraki, S., Mehrat, A., & Demirci, S. (2019). A Mobile Application for Wireless Attendance System.

[10] Lu, Q., Jiang, R., Ouyang, Y., Qu, H., & Zhang, J. (2020). BiRe : A client-side Bi-directional SYN Reflection mechanism against multi-model evil twin attacks. *Computers & Security 88*.

[11] Marques, N., Zuquete, A., & Barraca, J. P. (2019). Integration of the Captive Portal paradigm with the 802.1X architecture.

[12] Pomak, W., & Limpiyakorn, Y. (2018). Enterprise WiFi Hotspot Authentication with Hybrid Encryption on NFC-Enabled Smartphones. 247-250.

[13] Prakash, A., & Kumar, U. (2018). Authentication Protocols and Techniques: A Survey. *Authentication Protocols and Techniques: A Survey*.

[14] 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.

[15] Siregar, R. L. (2019). Implementasi Jaringan Hotspot dengan Captive Portal Zeroshell dan User Management LDAP. 87-96.

[16] Syarifudin, S., & Rahadjo, B. (2016). Perbandingan Teknologi Wireless untuk Sistem Absensi pada Smart University. *SENTER*, 37-45.

[17] Yanson, K. (2016). Results of implementing WPA2-enterprise in educational institution. *2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT).* Baku, Azerbaijan: IEEE.

[18] Zaim, S. (2015). APAKAH WPA/WPA2 BENAR-BENAR AMAN? DEKRIPSI PAKET DATA TERENKRIPSI PADA WPA/WPA2. *Seminar Nasional Informatika 2015* (pp. 268-276). Yogyakarta: UPN "Veteran".