Manajemen Dan Autentikasi Hotspot Menggunakan *Remote Access Dial-In User Service* (RADIUS) *Server* Pada Jurusan Teknik Komputer

Rizki Melia Asti[1)], Ema Laila[1)], Ali Fidaus[1)]
[1]Departemen Teknik Komputer, Politeknik Negeri Sriwijaya,
Jalan Srijaya Negara, Palembang, Sumatera Selatan 30139
e-mail: *rizkimeliaasti@gmail.com, emalaila@gmail.com, alifirdaus@gmail.com

Abstrak

Tujuan pembuatan laporan akhir ini yaitu untuk memanjemen dan mengautentikasi hotspot menggunakan remote access dial-in user service (RADIUS) server dengan RADIUS server dan dibantu dengan autentikasi berbasis token para pengguna harus memasukkan username serta token yang didapatkan melaui email pengguna sebelum menggunakan fasilitas hotspot, dengan begitu dapat menyulitkan user yang tidak terdaftar pada RADIUS server untuk masuk ke dalam jaringan. Administrator atau server jaringan akan dengan mudah melakukan manajemen terhadap siapa saja yang diizinkan untuk mengakses jaringan tersebut dengan menggunakan RADIUS User Manager dimana RADIUS User Manager akan memberikan kebijakan terhadap user.

Kata kunci*— Hotspot, Autentikasi, RADIUS, Mikrotik.*

Abstract

The purpose of this final report is to manage and authenticate hotspots using a remote access dial-in user service (RADIUS) server with a RADIUS server and assisted with token-based authentication, users must enter their username and token obtained via the user's email before using the hotspot, thus making it difficult for users who are not registered with the RADIUS server to enter the network. Network administrators or servers will easily manage who is allowed to access the network by using the RADIUS User Manager where the RADIUS User Manager will provide policies to users.

Keywords— *Hotspot, Authentication, RADIUS, Mikrotik*

1. PENDAHULUAN

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi jaringan *hotspot*. Dimana Jaringan *hotspot* ini menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan internet. Pada beberapa tahun terakhir ini pengguna jaringan *hotspot* mengalami peningkatan yang pesat. Dengan menggunakan teknologi *hotspot* kita dapat menikmati akses internet dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel. Keamanan pada hotspot juga sangat penting untuk menjaga dari kebocoran informasi maupun data.

Contoh implementasi jaringan *hotspot* di lembaga Pendidikan adalah di Jurusan Teknik Komputer Politeknik Negeri Sriwijaya. Peningkatan teknologi jaringan *hotspot* ini juga diimbangi dengan peningkatan pemakaian *hotspot* oleh mahasiswa di Jurusan Teknik Komputer. Akan tetapi penggunaaan jaringan *hotspot* ini masih sering di jumpai masalah yaitu

memungkinkan pengguna yang tidak berhak dapat masuk ke jaringan, koneksi yang tidak stabil, dan juga kurangnya manajemen jaringan.

Untuk mengatasi kendala ini, salah satu perangkat yang dapat digunakan adalah dengan *RouterBoard Mikrotik* yang didalamnya terdapat fitur *Remote Access Dial-in User Service* (RADIUS*) server*. *Remote Authentication Dial In User Service (RADIUS) Server* merupakan protokol jaringan yang menjalankan *service management Authentication*, *Authorization*, dan *Accounting* (AAA) secara terpusat untuk user yang terkoneksi dan hendak menggunakan *resource* dalam jaringan, dengan RADIUS *server* dan tipe autentikasi menggunakan token para pengguna harus memasukkan *username* serta token yang didapatkan melaui email pengguna sebelum menggunakan fasilitas *hotspot*, dengan begitu dapat menyulitkan *user* yang tidak terdaftar pada RADIUS server untuk masuk ke dalam jaringan. *Administrator* atau *server* jaringan akan dengan mudah melakukan manajemen terhadap siapa saja yang diizinkan untuk mengakses jaringan tersebut dengan menggunakan RADIUS *User Manager* dimana RADIUS *User Manager* akan memberikan kebijakan terhadap *user*.

Autentikasi adalah suatu metode untuk menentukan atau memastikan bahwa seseorang (atau sesuatu) adalah asli atau benar. Adapun proses validasi user pada saat memasuki sistem yaitu nama dan password dari user melalui proses pengecekan user pada suatu database yang diregistrasi sebelumnya oleh user itu sendiri. Pada sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses. Selain itu autentikasi juga merupakan salah satu dari banyak metode yang digunakan untuk membuktikan bahwa dokumen tertentu yang diterima secara elektronik asli datang dari orang yang bersangkutan dan tidak berubah keasliannya, dengan cara mengirimkan suatu kode tertentu melaui e-mail kemudian pemilik e-mail membalas e-mail tersebut [1].

Hotspot adalah sebuah wilayah terbatas yang dilayani oleh satu atau sekumpulan *Acces Point Wireless* LAN. Dimana pengguna dapat masuk ke dalam *Acces Poin*t secara bebas menggunakan perangkat sejenis *notebook*, laptop dan sebagainya [2].

RADIUS adalah *Remote Authentication Dial-in User Service* yang berfungsi untuk menyediakan mekanisme keamanan dan manajemen user pada jaringan computer [3].

RADIUS merupakan protokol *security* yang bekerja menggunakan sistem *client-server* terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan dari pengguna yang tidak berhak. RADIUS melakukan autentikasi *user* melalui serangkaian komunikasi antara *client* dan *server*. Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan layanan yang disediakan oleh jaringan [4].

UserManager merupakan fitur AAA *server* yang dimiliki oleh *MikroTik*. Sesuai kepanjangan AAA (*Authentication*, *Authorization* dan *Accounting*), *UserManager* memiliki *DataBase* yang bisa digunakan untuk melakukan autentikasi *user* yang *login* kedalam *network* kita, memberikan kebijakan terhadap *user* tersebut misalnya limitasi *transfer rate*, dan juga perhitungan serta pembatasan *quota* yang dilakukan *user* kita nantinya.

UserManager ini akan memudahkan kita yang ingin membuat layanan internet publik secara luas, misalnya *hotspot-hotspot* di *cafe*, *mall*, hotel dan sebagainya, karena dengan menggunakan *UserManager* ini kita cukup membuat 1 *account user*, dan *account user* tersebut bisa digunakan atau diakses dari *router-router Hotspot* yang sudah kita pasang [5].

2. METODE PENELITIAN

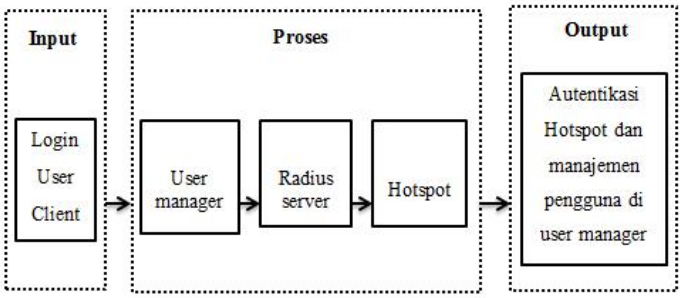
2.1 Tahapan Pengumpulan Data

Metode pengumpulan data yang dilakukan adalah dengan studi pustaka dan penelitian sejenis. Dalam tahapan ini dipelajari teori – teori yang terkait dengan topik penelitian yang dapat mendukung pemecahan masalah. Pencarian referensi dilakukan dengan membaca buku maupun mencari jurnal di internet dari hasil yang sudah pernah dikerjakan sebagai bahan perbandingan terhadap penelitian yang akan dikerjakan. Pustaka – pustaka yang dijadikan acuan dapat dilihat pada halaman daftar pustaka.

2.2 Tahapan Perancangan

Untuk perancangan sistem yang akan di bahas adalah mengenai bagaimana proses Memanajemen dan Mengautentikasi Hotspot Menggunakan *Remote Access Dial-In User Service* (RADIUS) *Server*. Berikut adalah diagram blok perancangan sistem dapat dilihat pada gambar 3.1.

2.2.1Diagram Blok



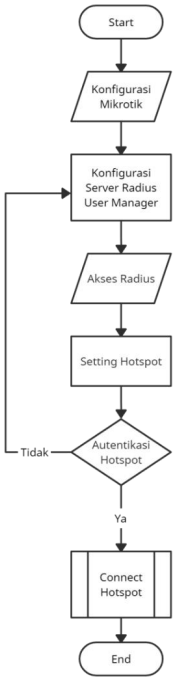
Gambar 2.1 Blok Diagram

Keterangan :

Login user client : login user client
User Manager : *package* yang harus ada dalam *router* mikrotik jika ingin mengaktifkan RADIUS *server*.
Radius Server : protokol jaringan yang menjalankan service management autentikasi secara terpusat.
Hotspot : sistem yang memberikan fitur autentikasi pada user yang akan menggunakan jaringan.

2.2.2 Flowchart

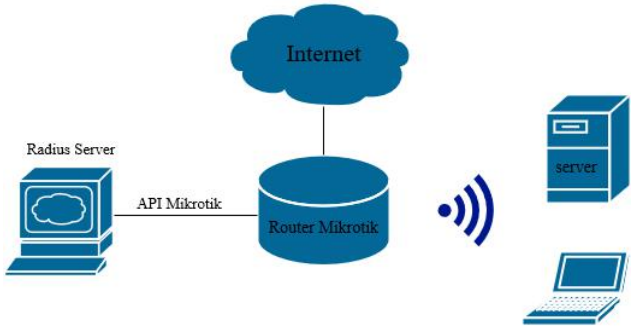
Berikut ini ialah diagram alir untuk proses *Remote Acces Dial-In User Service* (RADIUS) Server untuk Autentikasi Hotspot.



Gambar 2.2 *Flowchart*

2.2.3 Rancang Bangun Jaringan

Rancang bangun jaringan untuk *Remote Access Dial-In User Service* (Radius) *Server* pada *MikroTik* terlihat seperti pada gambar 3.3.



Gambar 2.3 Rancangan Jaringan

3. HASIL DAN PEMBAHASAN

3.1 Hasil dan Pembahasan Konfigurasi

3.1.1 Pengujian Koneksi Internet

Sebelum melakukan pengujian dan hasil, pastikan terlebih dahulu bahwa masing-masing ISP (Internet Service Provider) sudah terhubung dengan jaringan internet.

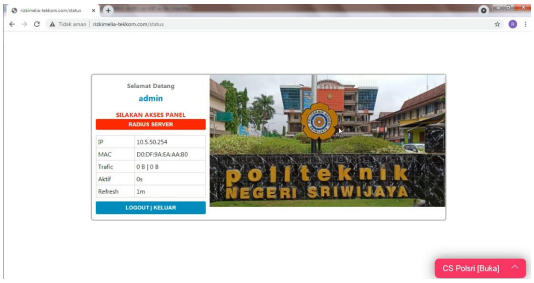
3.1.2 Hasil Konfigurasi Wireless

Setelah melakukan konfigurasi wireless lalu membuat SSID maka hasilnya SSID akan tampil pada menu hotspot artinya telah berhasil dibuat.

3.2 Hasil dan Pembahasan Manajemen Hotspot

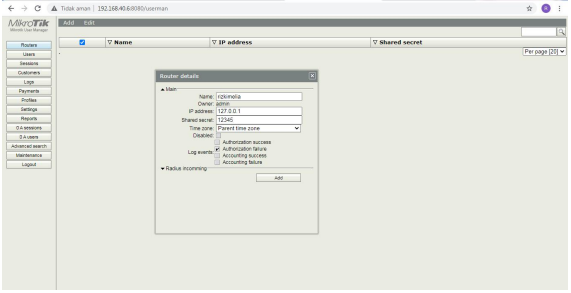
3.2.1 Manajemen Hotspot Pada RADIUS Server

Sebelum admin memanajemen hotspot di RADIUS *usermanager* admin harus menyambungkan ke *hotspot* yang telah dibuat sebelumnya, admin harus memasukan *username* dan *password* yang telah dibuat. Jika berhasil login hotspot maka akan ada panel RADIUS server *usermanager* dimana *admin* dapat memanajemen *user*.



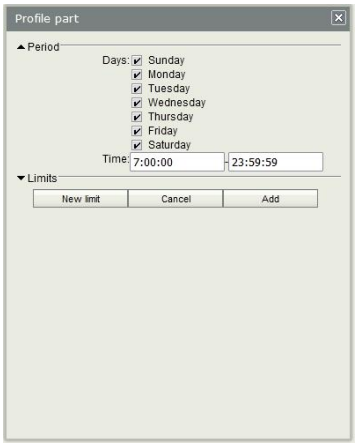
Gambar 3.1 Tampilan Login

Pada *usermanager* admin dapat mambahkan *routers. Router*s berfungsi untuk menginformasikan RADIUS, router mana saja yang boleh akses kedatabase.



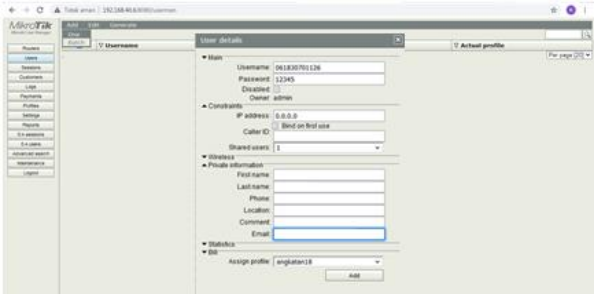
Gambar 3.2 Menambah Router

Lalu admin dapat membuat *Profile,* inilah yang menentukan ketentuan atau r*ole* suatu *user*. Admin juga dapat mengatur *limitation profile*, dimana pada bagian ini *admin* dapat mengatur hari, waktu *user*, jika *user* ingin menggunakan *hotspot* selain dari waktu dan hari yang ditentukan maka user tidak dapat mengakases *hotspot* tesebut dan dapat mengatur *rate limit* yang diinginkan.



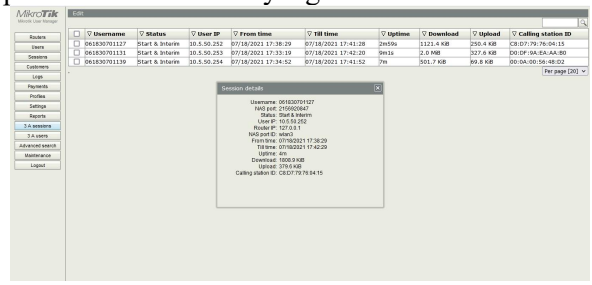
Gambar 3.3 Profile Part

Admin dapat membuat user isi *username*, password , *shared user*, lalu *private information user*.



Gambar 3.4 Add User

Pada menu *sessions admin* dapat memonitoring pengguna *hotspot*. Admin dapat mengetahui *sessions detail user* seperti *username* yang aktif, IP, waktu pemakaian, kecepatan *download* dan *upload.* Admin juga dapat melihat *username* yang aktif.

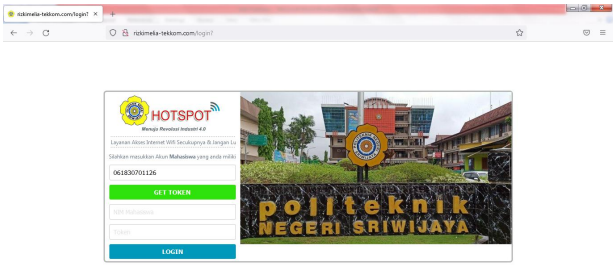


Gambar 3.5 Sessions

3.3 Hasil dan Pembahasan Autentikasi Hotspot

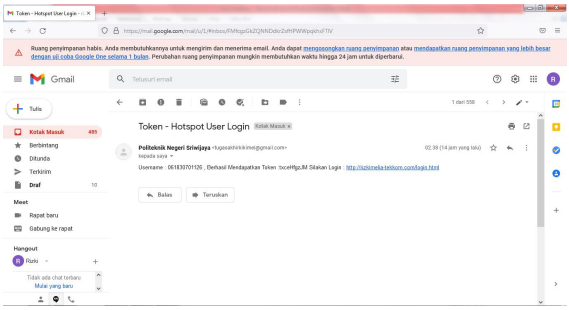
3.3.1 Autentikasi *Login* Hotspot

Autentikasi hotspot ini menggunakan token. Teknik keamanan ini mengautentikasi pengguna yang masuk ke jaringan menggunakan token keamanan yang disediakan oleh server. Autentikasi berhasil jika pengguna dapat membuktikan ke server bahwa ia adalah pengguna yang valid dengan melewati token keamanan. Silahkan masuk ke hotspot isi dengan NIM yang anda miliki, lalu klik *get* token untuk mendapatkan token.



Gambar 3.6 Halaman Login

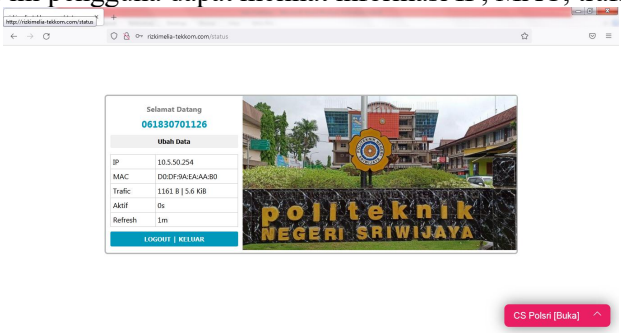
Lalu token anda akan dikirimkan melalui *email* yang sebelumya sudah terdaftar pada RADIUS *usermanager*. Terdapat pesan *username* dan token yang akan digunakan untuk masuk ke hotspot.



Gambar 3.7 Email

Setelah mendapatkan token di *email*, lalu klik *link login* yang diberikan. Maka akan masuk ke *web login*, lalu masukkan *username* dan token yang telah didapatkan pada *email*.

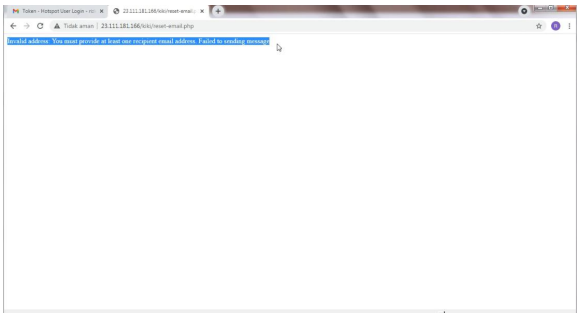
Jika sudah mendapatkan tampilan seperti dibawah ini artinya *hotspot* telah dapat digunakan pengguna. Pada menu ini pengguna dapat melihat informasi IP, MAC, traffic, Aktif, dan refresh.



Gambar 3.8 Login Berhasil

3.3.2 *Login Email* Tidak Terdaftar

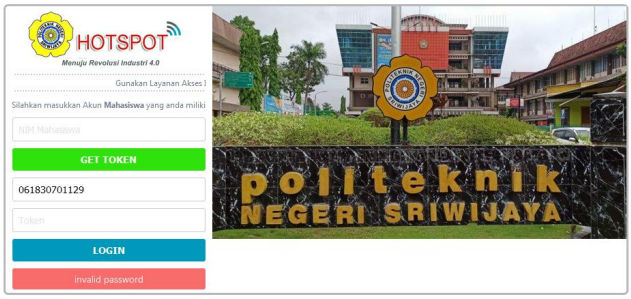
Jika *email* tidak terdaftar di RADIUS *usermanager*, maka pengguna akan mendapatkan pemberitahuan "*invalid address: You must provide at least one recipient email address. Failed to sending message*"



Gambar 3.9 Login Email Tidak Terdaftar

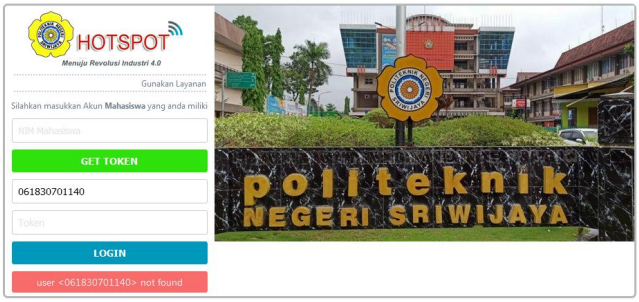
3.3.3 Login dengan *Username* dan Token Salah

Jika pengguna memasukkan token yang salah atau tidak terdaftar di RADIUS server maka akan muncul pemberitahuan bahwa token yang anda masukkan salah.



Gambar 3.10 *Invalid Password*

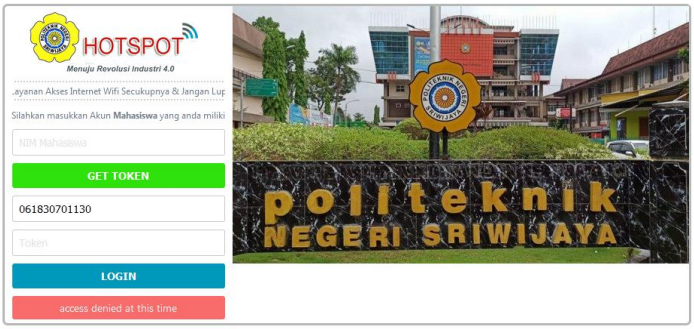
Begitu juga dengan nama pengguna yang salah atau tidak terdaftar, maka server menolak dengan memberitahu bahwa username tersebut tidak ditemukan.



Gambar 3.11 *Pengguna Tidak Terdaftar*

3.3.4 Waktu Pemakain *Hotspot*

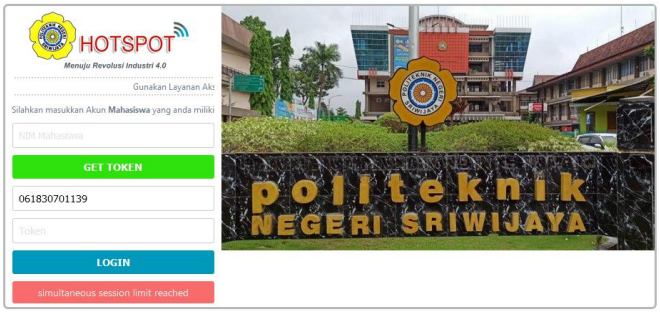
Pada saat *user* ingin *login* ke *hotspot* tetapi bukan jam dan waktu yang telah ditentukan *admin* maka akan mendapatkan pemberitahuan bahwa *"access denied at this time."*



Gambar 3.12 *User* Tidak Diizinkan *Login*

3.3.5 *Shared User Hotspot*

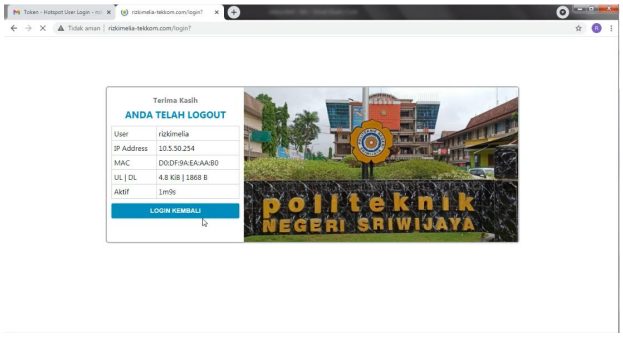
Hotspot ini hanya bisa digunakan oleh satu akun satu user, jadi jika ada user yang sedang menggunakannya juga server akan memberitahu bahwa *"simultaneous session limit reached"*.



Gambar 3.13 *Limit User*

3.3.6 *Log Out Hotspot*

Jika ingin keluar dari hotspot silahkan klik *logout*/keluar, jika tampilan sudah seperti gambar berarti anda telah berhasil logout dari hotspot dan anda sudah tidak dapat mengakses internet menggunakan hotspot ini.



Gambar 3.14 Tampilan Logout

4. KESIMPULAN

Berdasarkan hasil pembahasan dari Manajemen dan Autentikasi Hotspot Menggunakan *Remote Access Dial-In User Service* (RADIUS) *Server* maka dapat ditarik kesimpulan yaitu:

1. Autentikasi Hotspot menggunakan RADIUS Server dapat memfilter *user* yang tidak terdaftar di server untuk masuk ke dalam jaringan.
2. Autentikasi ini juga menggunakan token agar memperkuat keamanan hotspot
3. RADIUS Server dapat memanajemen user pada suatu jaringan, baik dari waktu pemakaian, jam pemakaian, penggunaan *bandwidth* dan sebagainya.

5. SARAN

Adapun saran untuk pengembangan lebih lanjut dari pembahasan yang telah dilakukan ialah penginputan data pribadi *user* dapat dilakukan secara otomatis agar tidak menyulitkan admin.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada jurusan teknik komputer politeknik negeri sriwijaya yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Pramartha. 2013. *Autentikasi User pada Jaringan.* Bandung: Informatika Bandung.

[2] Purbo, Onno W. 2006. *Buku pegangan internet wireless dan hotspot.* Jakarta: PT Elex media Komputindo

[3] Febyatmoko. 2006. *Otentikasi, Otorisasi & Pelaporan Koneksi User Wireless Chillispot Dan Server RADIUS.* (http://journal.uii.ac.id/index.php/mediainform diakses 20 Juni 2021)

[4] Hassel, J. 2002. R*ADIUS.* America: O'REILLY Media.

[5] Firdaus, Gilang. 2015. *Mikrotik.ID : Integrasi Hotspot dengan User Manager.* (http://www.mikrotik.co.id/artikel_lihat.php ?id=46, diakses tanggal 30 Juni 202)