Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

SISTEM KEAMANAN OTENTIKASI USER DENGAN NOTIFIKASI REALTIME MELALUI TELEGRAM BERBASIS DALORADIUS

Alfin Zidny Mandela [1], I Nyoman Buda Hartawan[2]
[12]*Program Studi Sistem Komputer, STMIK STIKOM Indonesia*
[1] *alfin.zidny@gmail.com,* [2]*buda.hartawan@stiki-indonesia.ac.id*

Received on	*Revised on*	*Accepted on*
14 Desember 2021	*11 Januari 2021*	*25 Januari 2021*

Abstract

The use of wireless network technology is rapidly increasing at this time causing problems in the security system. Ease of internet access through a wireless network, is also a security hole in the user authentication process. Various smart devices can be used to connect with only one account via the captive portal. In this research, a security system is designed to authenticate hotspot users with daloRADIUS-based telegram notifications. This system integrates hotspot routers, daloRADIUS servers and telegrams to improve the security system during the authentication process. Users are able to monitor the accounts they have used by any device. If there is a suspicious device, the user can also disconnect the device that uses his account to connect to the internet via the telegram application in realtime. Testing is done using the blackbox method by testing the ability of the system to carry out its functions. The test results show that the system is able to function properly and the user can control the use of the hotspot account that is owned through the telegram application in realtime

Keywords: *authentication user, daloRADIUS, telegram, security systems, hotspot*

Abstrak

Pemanfaatan teknologi jaringan wireless yang semakin pesat saat ini menimbulkan permasalahan dalam sistem keamanan. Kemudahan akses internet melalui jaringan wireless, juga menjadi celah keamanan dalam proses otentikasi user. Berbagai smart devices dapat digunakan untuk terkoneksi hanya dengan satu akun melalui captive portal. Pada penelitian ini dirancang sistem keamanan untuk otentikasi user hotspot dengan notifikasi telegram berbasis daloRADIUS. Sistem ini melakukan integrasi antara router hotspot, sever daloRADIUS, dan telegram dalam meningkatkan sistem keamanan saat proses otentikasi. User mampu memonitoring akun yang dimiliki telah digunakan oleh perangkat apa saja. Jika ada perangkat yang mencurigakan, user juga dapat memutuskan (kick) koneksi perangkat yang menggunakan akunnya untuk koneksi ke internet melalui aplikasi telegram secara realtime. Pengujian dilakukan menggunakan blackbox testing dengan menguji kemampuan sistem dalam menjalankan fungsinya. Hasil pengujian menunjukkan bahwa sistem mampu berfungsi dengan baik dan user dapat mengontrol penggunaan akun hotspot yang dimiliki melalui aplikasi telegram secara realtime.

Kata Kunci: *otentikasi user, daloRADIUS, telegram, sistem keamanan, hotspot*

---

1. PENDAHULUAN

Saat ini dunia sedang berada dalam era Revolusi Industri 4.0. Pemanfaatan teknologi digital menjadi semakin dekat dengan perusahaan maupun individu. Perangkat elektronik saat ini sudah dapat diintegrasikan dengan aplikasi komputer [1][2], bahkan dapat dikoneksikan melalui internet, yang lebih dikenal dengan Internet of Things[3][4][5]. Hal ini memungkinkan perangkat elektronik tersebut dikendalikan melalui aplikasi komputer ataupun smartphone, sehingga semakin mendorong perusahaan maupun pemerintah untuk menyediakan layanan internet. Setiap

perusahaan ataupun pemerintahan saat ini menyediakan layanan online yang memungkinkan masyarakat memperoleh informasi darimana saja dan kapan saja. Disamping itu juga, penggunaan perangkat smartphone untuk terkoneksi ke internet di Indonesia mencapai 93,9% setiap harinya [6]. Hal ini menunjukkan bahwa internet sudah menjadi kebutuhan dan sangat dekat dengan masyarakat. Selain kemudahan yang ditawarkan, internet juga memiliki resiko terhadap keamanan.

Perusahaan yang menyediakan layanan internet, umumnya melengkapi akses internet dengan sistem keamanan yang mengharuskan user melakukan otentikasi dengan cara login terlebih dahulu. Sistem ini biasa dikenal dengan *captive portal*. Otentikasi merupakan proses verifikasi awal terhadap *user* yang akan menggunakan sebuah sistem. Namun demikian, akun yang dimiliki oleh sebuah user dapat digunakan untuk login dengan lebih dari satu perangkat. Hal ini memberikan kemudahan sekaligus resiko bahaya jika terjadi penggunaan akun oleh user yang tidak berhak. Jika user memiliki lebih dari satu perangkat, maka setiap perangkat yang dimiliki dapat melakukan akses internet dengan akun yang sama. Namun apabila akun yang dimililki diketahui oleh orang lain, maka orang tersebut pun dapat menggunakannya. Apabila akun digunakan oleh user yang tidak berhak untuk melakukan tindakan kejahatan, maka yang tercatat pada sistem adalah pemilik akun yang sah. Sehingga bisa saja pemilik akun yang sah harus menanggung akibat dari kejahatan yang tidak dilakukannya. Hal ini terjadi karena pada umumnya, user tidak mengetahui akun yang dimilikinya sudah digunakan login oleh perangkat apa saja. Walaupun sistem administrator mengetahui perangkat yang login, namun tidak mengetahui pemilik dari perangkat tersebut.

Sistem keamanan yang umumnya diterapkan pada permasalahan diatas adalah dengan membatasi perangkat yang dapat menggunakan akun. Ini dapat dilakukan dengan cara membatasi jumlah perangkat maupun mendaftarkan MAC Address dari perangkat yang akan terkoneksi ke internet. Kelemahan dari metode ini adalah user harus menggunakan perangkat yang terdaftar untuk terkoneksi ke internet. Jika user melakukan penggantian perangkat, maka harus mendaftarkan ulang perangkat tersebut. User hanya bisa mengakses internet menggunakan perangkat yang sudah terdaftar saja.

Radius merupakan salah satu protokol jaringan yang digunakan dalam melakukan manajemen user hotspot[7]. Radius mampu diintegrasikan dengan router hostpot mikrotik dan menjadi satu kesatuan dalam manajemen user hotspot. Subandri, dkk dalam penelitiannya melakukan sistem otentikasi dan otorisasi untuk proses login multi aplikasi mikhmon dengan mengoptimalkan penggunaan dari radius server[8]. Kuswanto pada penelitiannya menggunakan Radius dalam melakukan manajemen user hotspot pada mikrotik[9]. Walaupun demikian, penggunaan Radius masih berdiri sendiri dengan menggunakan router hotspot mikrotik. Pada penelitian ini dilakukan penerapan daloRADIUS dengan integrasi aplikasi telegram untuk memberikan notifikasi kepada pengguna tentang penggunaan user yang dimiliki. Pengguna nantinya mampu melakukan monitoring dan kontrol terhadap user hostpot yang dimiliki. Aplikasi telegram dapat digunakan untuk melakukan monitoring sistem atau jaringan[10][11][12].

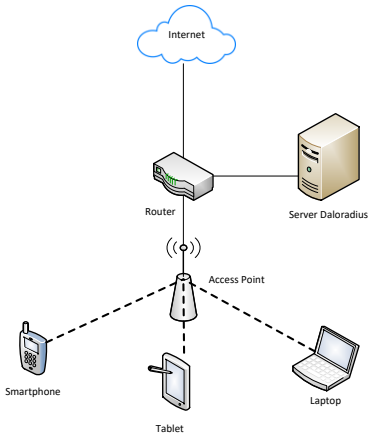
Pada penelitian ini dilakukan perancangan sistem keamanan otentikasi user dengan notifikasi telegram berbasis daloRADIUS. Sistem ini memungkinkan user mengontrol penggunaan akun yang dimiliki untuk otentikasi akses ke internet melalui aplikasi telegram. Jika akun yang dimiliki digunakan untuk login, maka secara *real time* user akan mendapatkan notifikasi melaui telegram, bahwa akun yang dimiliki digunakan untuk login. User dapat melakukan pilihan kick/membatalkan proses login jika tidak mengetahui perangkat yang menggunakan akunnya. Disamping itu juga, user dapat melakukan penggantian password akun yang dimiliki secara realtime melalui aplikasi telegram. Penelitian dilakukan pada user mikrotik dengan pemanfaatan server daloRADIUS. Hal ini dilakukan mengingat banyaknya penggunaaan

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

perangkat mikrotik sebagai router hotspot untuk akses internet baik di perusahaan swasta maupun pemerintah. Sedangkan daloRADIUS digunakan karena memiliki kemampuan dalam pengelolaan user hotspot, dan dilengkapi dengan sistem pelaporan, serta pencatatan aktivitas (accounting). Disamping itu daloRADIUS menggunakan bahasa pemgrograman PHP dan JavaScript memungkinkan sehingga dapat diintegrasikan dengan sistem database seperti MySQL, PostgreSQL, Sqlite, dan MsSQL.

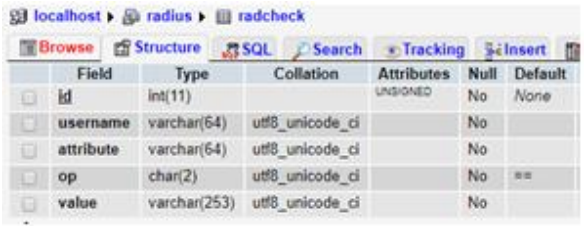
2. METODE

Pada penelitian ini dilakukan eksperimen meggunakan perangkat jaringan komputer seperti router mikrotik, access point, server untuk daloRADIUS, dan smartphone yang diinstalasi aplikasi telegram. Gambar 1 menunjukkan topologi jaringan yang digunakan pada penelitian ini.



Gambar 1 Topologi Jaringan

Konfigurasi hotspot-server pada router mikrotik diintegrasikan dengan server daloRADIUS sebagai manajemen user. Pada server daloRADIUS harus dilakukan konfigurasi untuk secret karena mikrotik akan terhubung ke server melalui address dan secret pada server. Untuk konfigurasi address dan secret dapat diakses melalui nano /etc/freeradius/clients.conf. Pada platform Daloradius sudah terinstall phpMyAdmin yang berfungsi untuk membuat username dan password yang tersimpan pada tabel radcheck.

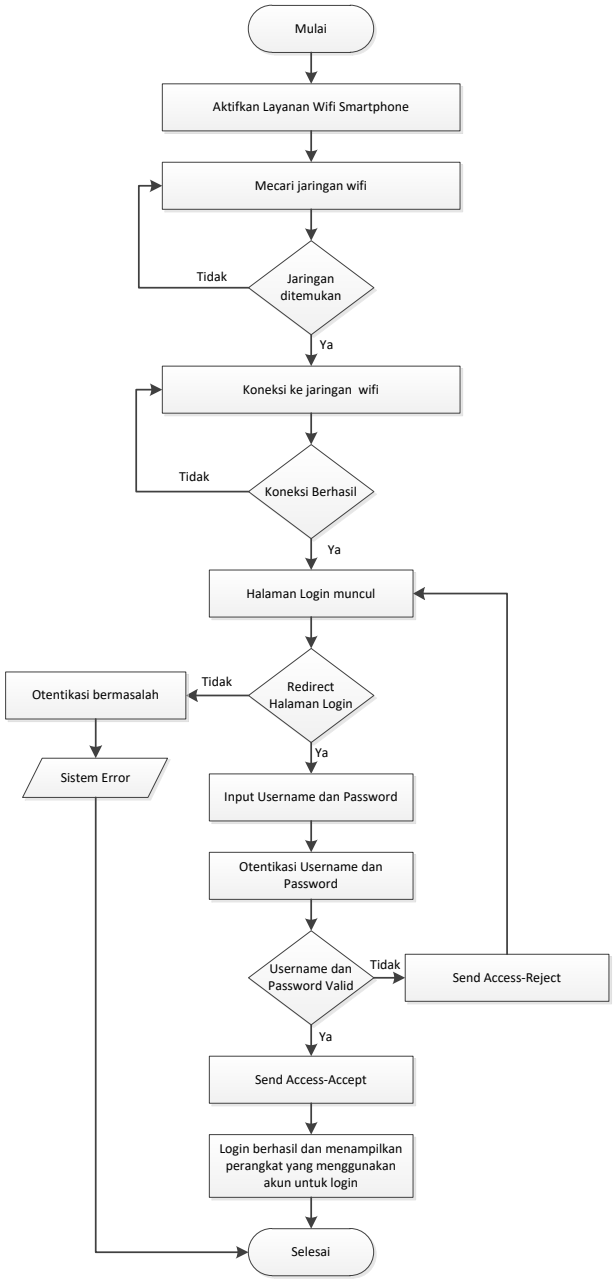


Gambar 2 Struktur Tabel Radcheck

Cara kerja dari sistem yang dibangun adalah sebagai berikut 1) Pengguna terhubung kedalam jaringan Wi-Fi dan pengguna mendapatkan IP Address secara otomatis dari router; 2) Setelah terkoneksi dengan jaringan Wi-Fi dan mendapatkan IP Address pada perangkat pengguna, secara otomatis router akan melakukan proses routing dari network ke alamat network pada server; 3) Pengguna akan login melalui *Captive Portal*. *Captive Portal* ini merupakan gateway router yang sudah dilakukan konfigurasi sebelumnya; 4) *Login page*

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

secara otomastis muncul dimana pengguna diminta untuk memasukkan *username* dan *password*; 5) Pengguna harus login ke dalam jaringan Wi-Fi menggunakan *username* dan *password* yang sudah diperoleh sebelumnya; 6) Pada saat pengguna melakukan *login* menggunakan *username* dan *password*, proses yang terjadi adalah *username* dan *password* yang digunakan dikirim ke server daloRADIUS oleh router; 7) Server akan melakukan pengecekan melalui proses *query database* pada tabel radcheck; 8) Jika status pada radcheck bernilai *access-accept* maka secara otomatis proses login berhasil; 9) Namun jika status pada radcheck bernilai *accept-reject* maka login gagal; 10) Jika proses login berhasil maka tampilan selanjutnya adalah menampilkan ifor*username* untuk *login* yang digunakan sudah dipakai oleh perangkat apa saja.



Gambar 3 Flowchart Sistem

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

Untuk mejelaskan cara kerja sistem yang dibangun, pada penelitian ini dibuatkan flowchart sistem. Gambar 3 menujukkan flowchart dari sistem yang dibangun.

3. HASIL DAN PEMBAHASAN

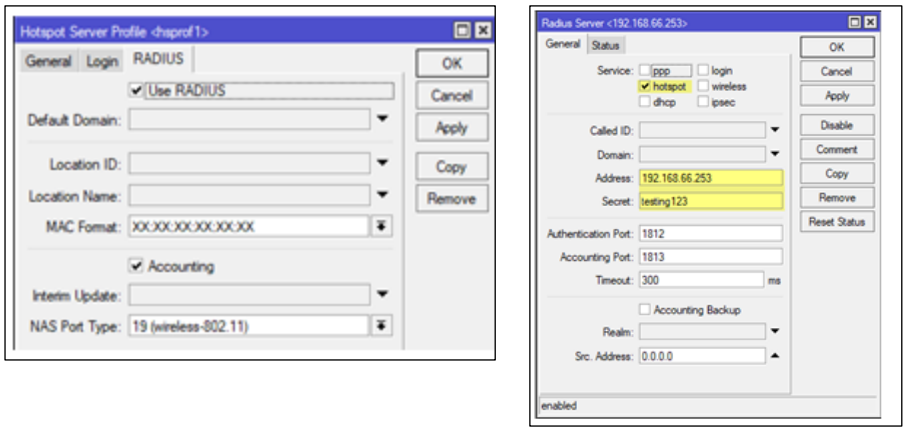
Implementasi dari penelitian yang dilakukan menggunakan perangkat mikrotik, *access point*, dan sebuah server daloRADIUS serta aplikasi telegram sebagai notifikasi.

Router mikrotik secara otomatis akan membuat file pada saat melakukan konfigurasi Hotspot Server. Kumpulan file hotspot akan ditampung secara otomatis pada menu Files di winbox. Halaman login hotspot akan disimpan dan dimunculkan oleh login.html secara default. Karena dalam penelitian ini login mikrotik dengan login daloRADIUS akan diintegrasikan, maka konfigurasi perlu dilakukan pada halaman login.html.

```
<html>
<title>...</title>
<body>
<form name="redirect" action="http://192.168.66.253/loginpage/redirect.php" method="post">
<input type="hidden" name="mac" value="$(mac)">
<input type="hidden" name="ip" value="$(ip)">
<input type="hidden" name="username" value="$(username)">
<input type="hidden" name="link-login" value="$(link-login)">
<input type="hidden" name="link-orig" value="$(link-orig)">
<input type="hidden" name="error" value="$(error)">
<input type="hidden" name="chap-id" value="$(chap-id)">
<input type="hidden" name="chap-challenge" value="$(chap-challenge)">
<input type="hidden" name="link-login-only" value="$(link-login-only)">
<input type="hidden" name="link-orig-esc" value="$(link-orig-esc)">
<input type="hidden" name="mac-esc" value="$(mac-esc)">
</form>
<script language="JavaScript">
    document.redirect.submit();
</script>
</body>
</html>
```

Gambar 4 Konfigurasi Login.html

Link untuk proses redirect ke halaman login yang ada pada server radius. Fungsi dari file redirect.php adalah mengarahkan dari router ke halaman login. File redirect.php ini terlebih dahulu membaca konfigurasi pada config.php. Proses pembacaan awal konfigurasi hotspot antar router dengan server ada pada file config.php. File ini berfungsi melakukan pembacaan file database yang tersimpan dalam server, pembacaan file – file yang berada pada server yang tersimpan di folder loginpage, kemudian dilakukan pembacaan lagi oleh gateway router dan selanjutnya mengarahkan kembali ke halaman login router.



Gambar 5 Konfigurasi Radius pada Mikrotik

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

Gambar 6 menunjukkan konfigurasi radius pada router hotspot mikrotik. Konfigurasi ini bertujuan untuk mengaktifkan fungsi radius pada router hotspot mikrotik, sehingga mampu diintegrasikan dengan database eksternal pada server daloRADIUS.

Penelitian ini memiliki tujuan utama yaitu untuk memberitahukan kepada pengguna jaringan hotspot, bahwa otentikasi yang diberikan admin jaringan hanya boleh digunakan oleh device user yang bersangkutan, dan jika ada yang memakai otentikasi tersebut tanpa ijin dari pengguna yang berhak, maka akan memberikan notifikasi secara realtime. Pada penelitian ini notifikasi dikirimkan menggunakan aplikasi telegram.

Konfigurasi dilakukan dengan menghubungkan jaringan hotspot dan aplikasi telegram. Terlebih dahulu pada aplikasi telegram dibuat Bot Server. Bot Server ini berfungsi untuk memberikan informasi kepada setiap user yang konek kedalam jaringan hotspot yang disediakan. Proses selanjutnya adalah membuat konektivitas antara server dan telegram dengan memasukkan akses HTTP API kedalam scheduler.

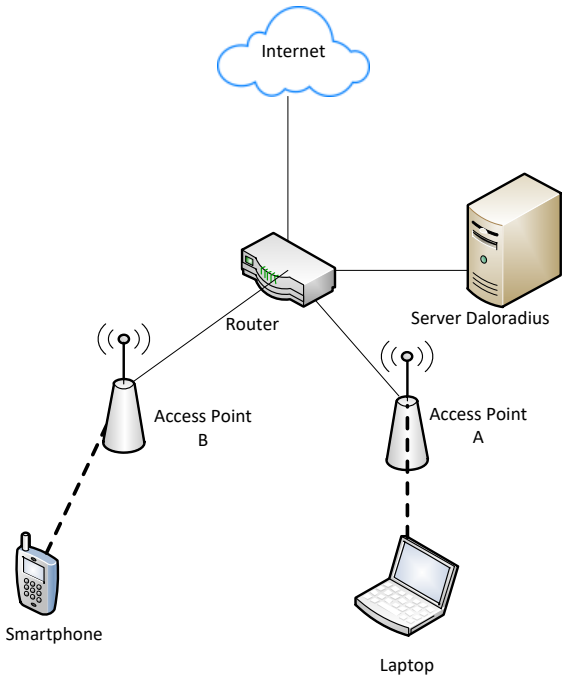
Gambar 6 Verifikasi No Hp Alfindev_bot

Untuk mendapatkan notifikasi secara realtime user diwajibkan untuk menambahkan Alfindev_bot ke dalam pertemanan telegram, dengan cara mencari dalam pencarian Alfindev_bot. Setelah ditambahkan kekontak telegram, user bisa memulai dengan /start dan memverifikasi no hp yang sudah didaftarkan pada saat registrasi awal untuk mendapatkan otentikasi.

Gambar 7 menunjukkan bahwa nomor hp yang digunakan untuk menerima notifikasi tentang penggunaan user hotspot sudah berhasil diverifikasi. Apabila user hotspot digunakan untuk melakukan akses internet, maka pengguna akan langsung menerima notifikasi.

Setelah konfigurasi dilakukan selanjutnya dilaksanakan pengujian terhadap sistem yang dibangun. Pada pengujian pertama dilakukan menggunakan 1 access point sebagai media Wi-Fi. Kemudian dihubungan 2 buah *smart devices* ke jaringan Wi-Fi melalui access point tersebut, dan menggunakan otentikasi yaitu dengan username dan password yang sama. Selanjutnya digunakan dua buah access point A dan B untuk dapat terkoneksi ke internet. Masing-masing smart devices terkoneksi menggunakan access point yang berbeda namun akun saya sama. Hasil pengujian yang dilakukan menunjukkan bahwa kedua smart devices yang digunakan dapat berhasil login dan mengakses internet.

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index



Gambar 7 Topologi dengan 2 Access Point

Gambar 8 merupakan topologi dengan 2 access point untuk terkoneksi ke internet. Satu perangkat dikoneksikan ke Access Point A dan perangkat yang lainnya dikoneksikan dengan Access Point B. Untuk login menggunakan username dan password yang sama oleh kedua perangkat. Pengujian ini bertujuan untuk mengetahui kemampuan sistem dalam mendeteksi jumlah perangkat yang digunakan untuk login menggunakan username dan password yang sama.Pada halaman login nantinya akan muncul jumlah perangkat yang digunakan untuk login oleh user yang dapat dilihat pada Gambar 10.

Tabel 1 Pengujian Akses Login User Hotspot

Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
Login dengan menggunakan username dan password yang terdaftar	Berhasil login dengan username dan password yang terdaftar	Valid
Login dengan menggunakan username dan password yang tidak terdaftar	Gagal melakukan login dengan mendapat informasi username atau password salah	Valid
Setelah berhasil login muncul halaman ganti password	Muncul halaman ganti password	Valid
Pada halaman ganti password jika di klik lewati maka akan muncul halaman Login Success	Muncul halam Login Success	Valid

Pengujian pertama dilakukan terhadap akses login user hotspot. Pada Tabel 1 dapat dilihat pengujian dari fungsi akses login yang dilakukan. Pengujian ini dilakukan dengan mengkoneksikan perangkat ke access point menggunakan username dan password yang terdaftar, dan yang tidak terdaftar. Hal ini dilakukan untuk mengetahui respon dari sistem ketika

Jurnal Krisnadana
Volume 1 Number 2, Januari 2022
e-ISSN 2808-3563 p-ISSN 2808-3520
https://ejournal.catuspata.com/index.php/jkdn/index

terdapat user yang login dengan username dan password terdaftar, dan tidak terdaftar. Pengujian dilakukan dengan metode blackbox yang ditunjukkan pada Tabel 1. Hasil pengujian menunjukkan bahwa akses login user hotspot dapat berfungsi dengan baik sehingga diberikan status valid yang berarti bahwa output yang dihasilkan oleh sistem sesuai dengan yang direncanakan. Sehingga akses login user hostpot dinyatakan dapat berfungsi dengan baik dan sesuai harapan.

Pengujian yang dilakukan selanjutnya adalah user melakukan pemutusan (kick) koneksi yang dilakukan oleh smart devices. Ketika user digunakan untuk login oleh smart devices, maka pengguna akan menerima notifikasi melalui telegram secara realtime.

Gambar 8 Notifikasi berhasil login

Gambar 9 diatas merupakan notifikasi yang dikirimkan melalui telegram kepada pengguna tentang penggunaan user yang dimiliki. Pengguna dapat mengklik link yang dikirimkan tersebut dan melihat perangkat yang terkoneksi. Jika perangkat tersebut tidak dikenal, pengguna dapat langsung melakukan “kick” untuk memutus koneksi internet pada perangkat tersebut.

Gambar 9 Informasi Otentikasi Lebih dari 1 Device

Gambar 10 menunjukkan informasi otentikasi menggunakan lebih dari 1 perangkat yang dapat di “kick” karena merupakan perangakt yang tidak dikenal oleh pengguna.

Jurnal Krisnadana
Volume x Number x, Bulan Tahun
e-ISSN 0000-0000 p-ISSN 0000-0000
https://ejournal.catuspata.com/index.php/jkdn/index

Tabel 2 Pengujian notifikasi dan kontrol penggunaan akun melalui telegram

Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
Telegram mengirimkan Link untuk melihat aktif user	Telegram mengirimkan link	Valid
Jika Link Telegram di klik oleh user, maka akan menampilkan halaman aktif user	Tampil halaman aktif user	Valid
Halaman tampil user aktif memberikan action Kick user	Memberikan action kick	Valid
Fitur Kick user berfungsi untuk memutuskan device dari jaringan internet	Device terputus dari jaringan	Valid
Jika action kick di klik maka device akan terputus dan muncul halaman login lagi	Muncul halaman login	Valid
Otentikasi digunakan login lebih dari 1 device	Halaman informasi aktif user muncul semua device dengan otentikasi yang sama	Valid

Tabel 2 menunjukkan hasil pengujian yang dilakukan terhadap fungsi sistem dalam mengirimkan notifikasi dan kontrol terhadap penggunaan user hotspot. Hasil pengujian menunjukkan seluruh rencana pengujian yang dilakukan berjalan dengan baik yang berarti bahwa sistem mampu berfungsi sesuai dengan yang diharapkan, sehingga diberikan status valid. Sistem mampu memberikan notifikasi melalui telegram ketika ada pihak yang menggunakan user untuk login hotspot, dan mampu memutuskan koneksi internet ketika terdapat pihak yang tidak berhak telah menggunakan user yang dimiliki. Pemutusan koneksi dapat dilakukan dengan menggunakan perintah “kick” melalui instagram.

Gambar 10 Notifikasi Penggantian Password

Selain mampu memutuskan koneksi internet, pengguna juga mampu melakukan control penggantian password yang dimiliki melaui telegram. Ketika pengguna atau pihak

lain mencoba untuk melakukan penggantian password, maka terlebih dahulu akan dikirimkan notifikasi melalui telegram, dan pengguna harus melakukan verifikasi melalui aplikasi telegram untuk menyetujui atau membatalkan penggantian password.

Gambar 11 menunjukkan notifikasi yang diterima oleh pengguna ketika pengguna atau pihak lain mencoba melakukan penggantian password. Konfirmasi penggantian password juga bisa dibatalkan jika penggantian password tidak dikehendaki. Prosesnya adalah pada saat telegram mengirimkan konfirmasi pergantian password ketikkan “NO” untuk pembatalan. Hal ini menyebabkan akun pengguna menjadi lebih aman karena membutuhkan verifikasi terlebih dahulu sebelum dilakukan penggantian password.

Tabel 3 Pengujian notifikasi dan kontrol penggantian password melalui telegram

Skenario Pengujian	Hasil yang diharapkan	Hasil Pengujian
Pada halaman ganti password jika textbox ganti password diisi dan klik oke, maka aka n ada konfirmasi ke telegram terlebih dahulu	Konfirmasi telegram realtime	Valid
Konfirmasi pergantian password pada telegram ada pilihan Yes dan No	Pilihan konfirmasi	Valid
Jika konfirmasi dalam telegram dipilih yes, maka password akan otomatis diganti pada server	Password berhasil diganti pada server	Valid
Jika konfirmasi dalam telegram dipilih no, maka password akan otomatis diganti pada server	Password tidak berhasil diganti pada server	Valid
Halaman Login Success Menampilkan device yang dipakai dari otentikasi yang digunakan	Menampilkan device dari otentikasi yang digunakan	Valid
Ketika Login sukses maka Telegram akan mengirimkan notifikasi kepada user bahwa otentikasi yang dimiliki digunakan untuk login kedalam jaringan	Telegram mengirimkan pesan kepada user	Valid

Tabel 3 merupakan hasil pengujian dalam memberikan notifikasi kepada pengguna apabila terdapat pihak yang melakukan penggantian password. Ketika pengguna ataupun pihak lain yang mencoba melakukan penggantian password, maka terlebih dahulu sistem akan mengirikan notifikasi kepada pengguna melalui telegram. Pengguna dapat menyetujui atau menolak penggantian password tersebut. Hasil pengujian menunjukkan bahwa sistem mampu berfungsi sesuai dengan yang diharapkan sehingga diberikan status valid. Selain itu sistem juga mampu menampilkan perangkat yang digunakan untuk terkoneksi ke internet.

KESIMPULAN DAN SARAN

Sistem hotspot mikrotik dapat menggunakan database secara eksternal untuk penyimpanan informasi otentikasi, dengan memanfaatkan DaloRADIUS sebagai server. Dalam sistem integrasi hotspot pada mikrotik dengan radius server berbasis daloRADIUS, mampu meningkatkan keamanan otentikasi yang memungkinkan user untuk melakukan

monitoring terhadap akun hotspot yang dimiliki. User mampu menerima notifikasi secara realtime melalui aplikasi telegram ketika ada pihak lain yang menggunakan akun yang dimiliki untuk proses otentikasi. User juga dapat mengganti password akun tanpa harus meminta bantuan administrator jaringan. Dari hasil pengujian blacbox yang dilakukan, secara keseluruhan sistem dapat berfungsi dengan baik.

REFERENSI

[1] I. G. M. N. Desnanjaya, I. B. A. I. Iswara, A. A. G. Ekayana, P. P. Santika, and I. N. B. Hartawan, "Automatic high speed photography based microcontroller," *J. Phys. Conf. Ser.*, vol. 1469, no. 1, 2020.

[2] A. A. G. Ekayana, I. N. B. Hartawan, I. G. M. N. Desnanjaya, and I. D. M. A. B. Joni, "Body mass index measurement system as a desktop-based nutrition monitor," *J. Phys. Conf. Ser.*, vol. 1469, no. 1, 2020.

[3] D. Bruneo *et al.*, "An IoT service ecosystem for Smart Cities: The #SmartME project," *Internet of Things*, vol. 5, pp. 12–33, 2019.

[4] P. Jariyayothin, K. Jeravong-Aram, N. Ratanachaijaroen, T. Tantidham, and P. Intakot, "IoT Backyard: Smart watering control system," *Proceeding 2018 7th ICT Int. Student Proj. Conf. ICT-ISPC 2018*, pp. 1–6, 2018.

[5] I. N. B. Hartawan and I. W. Sudiarsa, "Analisis Kinerja Internet of Things Berbasis Firebase Real-Time Database," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 2, no. 1, pp. 6–17, 2019.

[6] APJII, "Penetrasi & Profil Perilaku Pengguna Internet Indonesia Tahun 2018," *Apjii*, p. 51, 2019.

[7] S. Pengajar, T. Elektro, F. Teknik, and U. Udayana, "Implementasi Sistem Autentikasi Jaringan Hotspot Universitas Udayana Dengan Menggunakan Open Source Freeradius," *Maj. Ilm. Teknol. Elektro*, vol. 9, no. 1, 2010.

[8] S. Hanadwiputra, S. Subandri, and P. K. Murti, "Optimalisasi Radius Server Sebagai Sistem Otentikasi Dan Otorisasi Untuk Proses Login Multi Aplikasi Mikhmon Menggunakan," *Semin. Nas. Inform. 2011*, vol. 2011, no. semnasIF, pp. 17–23, 2011.

[9] H. Kuswanto, "Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router Herman," *Sist. Autentikasi Hotspot Menggunakan Radius Serv. Mikrotik Router Herman*, vol. 2, no. 1, pp. 43–50, 2017.

[10] B. Rifai, N. Nuryadi, and A. Ripai, "Implementasi Telegram Notification Alert Pada Network Monitoring System Dengan Nagios," *J. Mantik Penusa*, vol. 3, no. 3, pp. 54–60, 2019.

[11] F. Panjaitan *et al.*, "Pemanfaatan Notifikasi Telegram Untuk Monitoring," vol. 10, no. 2, pp. 725–732, 2019.

[12] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram sebagai Notifikasi Serangan untuk Jaringan Forensik," *Query J. Inf. Syst.*, vol. 1, no. 2, pp. 6–14, 2017.