

PERANCANGAN SISTEM KEAMANAN JARINGAN HOTSPOT MIKROTIK ROUTER OS LOGIN MENGGUNAKAN ONE-TIME PASSWORD (OTP)

Khairullah, M Yoan Joupin, Marhalim, A.R. Walad Mahfuzhi

Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Jalan Bali, Teluk Segara, Kota Bengkulu, Indonesia
hunterant18@gmail.com

ABSTRAK

Pada teknologi jaringan semakin banyak pengguna, maka diperlukan manajemen jaringan. Karena era digital saat ini, kebutuhan akan akses internet yang cepat, aman, dan efisien sangat penting, terutama di lingkungan kampus, perkantoran, dan area publik lainnya. Hal ini dikarenakan Keamanan menjadi salah satu aspek penting yang harus diperhatikan. *Hotspot* merupakan media pendistribusi internet berbasis nirkabel yang memiliki sistem autentikasi untuk penggunaannya. Tujuan dari penelitian ini mengangkat permasalahan mengenai keamanan informasi *password* dari jaringan *hotspot*. Mudah-mudahan data diperoleh melalui internet sepatutnya diimbangi dengan jaminan kerahasiaan data dari orang-orang yang tidak berkepentingan, dengan menggunakan *One-time Password (OTP)* untuk pengamanan data pada sistem login *hotspot* sehingga memberikan akses internet secara tepat dan hanya bagi pengguna yang memiliki *One-time Password (OTP)*. Penelitian ini dilakukan berdasarkan hasil studi kasus pada UP-TIK Universitas Muhammadiyah Bengkulu. Menggunakan Metode Otentikasi pengguna (*user*) dan Menggunakan *One-time Password (OTP)* Sehingga memberikan user kepada pengguna sah dan memberikan serangkaian *password* acak yang hanya dapat digunakan sekali dalam periode waktu tertentu serta menerapkan kebijakan akses yang lebih ketat untuk meningkatkan keamanan jaringan. Hasil Penelitian dengan metode ini diharapkan sistem keamanan jaringan *hotspot* dapat berjalan dengan baik, dan Keamanan jaringan lebih aman dari sebelumnya. Kesimpulan yaitu, penelitian ini berhasil merancang dan membangun jaringan *hotspot* pada UP-TIK menjadi lebih stabil dan keamanan jaringan lebih aman dari pengguna asing karena sudah diberikan user untuk pengguna sah dan memberikan *password* sekali pakai.

Kata Kunci : Mikrotik, *One-time Password (OTP)*, Authentication

1. PENDAHULUAN

Hotspot adalah salah satu solusi yang banyak digunakan untuk menyediakan akses internet nirkabel (*Wi-Fi*) di berbagai lokasi publik seperti kampus, kafe, hotel, dan perkantoran. Dengan adanya jaringan *hotspot*, pengguna dapat mengakses internet dengan mudah menggunakan perangkat nirkabel seperti laptop, smartphone, atau tablet.

Berdasarkan hasil survei, tantangan yang sering dihadapi dalam pengelolaan keamanan jaringan *hotspot* mencakup berbagai aspek. Salah satunya adalah pentingnya menjaga keamanan sistem informasi. Tanpa sistem keamanan yang baik, penggunaan internet dapat menjadi tidak efektif dan efisien, terutama ketika banyak pengguna mengakses jaringan secara bersamaan. Hal ini dapat menyebabkan kecepatan akses internet menjadi lambat dan mengurangi kenyamanan pengguna.

Metode Otentikasi pengguna dalam jaringan yaitu proses verifikasi pengguna sebelum mereka diberikan akses ke jaringan. Dalam konteks manajemen *bandwidth* menggunakan perangkat Mikrotik, otentikasi pengguna bertujuan untuk memastikan bahwa hanya pengguna yang sah dan terdaftar yang dapat mengakses jaringan *hotspot*, serta untuk Mengatur serangkaian *password* acak yang hanya dapat digunakan sekali dalam periode waktu tertentu.

Maka dari itu, yang melatar belakangi penelitian ini, yaitu dari hasil survey di UP-TIK

Universitas Muhammadiyah Bengkulu yang menunjukkan bahwa adanya pengguna asing pada jaringan *hotspot* yang ada, sehingga tidak selalu memberikan akses internet yang lambat, terutama saat terjadi peningkatan jumlah pengguna. Koneksi yang buruk di beberapa perangkat menyebabkan pengguna sah mengalami kesulitan mengakses internet. Untuk mengatasi masalah ini, peneliti menggunakan metode "Otentikasi Pengguna (*user*)" menggunakan *One-Time Password (OTP)* untuk memperkuat keamanan akses internet. Metode ini melibatkan pembagian kelompok pengguna dan memberikan *password* sekali pakai untuk memastikan akses internet yang stabil dan terbatas hanya untuk pengguna yang sah.

Penelitian ini bertujuan untuk Keamanan jaringan *hotspot* agar tidak ada pengguna asing yang memakai jaringan kita. Dimana *user* akan menggunakan Jaringan *Hotspot* tersebut harus mendapat kode *password* dari server yang berasal dari *Google Authentication* dan memberikan *password user* yang berbeda-beda baik dari user yang sama maupun user yang berbeda. Di harapkan mampu memperkuat keamanan jaringan dan mengurangi penyalahgunaan internet di jaringan *hotspot* kita.

2. TINJAUAN PUSTAKA

Pada Penelitian sebelumnya tentang menambah keamanan *one-time password*, salah satunya adalah penelitian yang dilakukan oleh E.Kalaikavitha dan Juliana gnanaselvi yang berjudul "Secure Login Using Encrypted One Time Password (OTP) and Mobile Based

Login Methodology” dengan cara mengenkripsi OTP dengan menggunakan algoritme AES dan kesimpulan yang didapatkan adalah mengenkripsi OTP dengan algoritme AES memberikan tambahan keamanan pada OTP tersebut.[1]

2.1. Penelitian Terkait

Pada Penelitian terdahulu dengan judul “Implementasi *One Time Password* dengan Metode *Advanced Encryption Standard*” Metode OTP akan diterapkan pada smartphone dengan menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES), Dikenal sebagai cipher yang aman untuk melindungi data rahasia, algoritma AES juga dapat diintegrasikan ke dalam aplikasi yang memerlukan tingkat keamanan tinggi. Untuk menghasilkan OTP, AES lebih fleksibel dan memiliki kinerja lebih cepat dibandingkan dengan penggunaan hash function.[2]

Pada Penelitian Tedahulu Brajesh Kumar Kushwaha (2012), telah melakukan penelitian tentang *An Approach for User Authentication One Time Password (Numeric And Graphical)* membahas tentang skema pembuatan password satu kali pakai (OTP) dengan 5 memadukan antar gambar dan karakter. Penggunaan gambar dalam penginputan *password* akan membantu pengguna dalam mengingat *password* yang telah dibuat. Tetapi di dalam penelitian ini tidak begitu jelas skema pembuatan atau generate *password* otp yang dilakukan.[3]

2.2. Mikrotik

Mikrotik berasal dari kata “*mikrotiks*” bahasa Latvia yang berarti “jaringan kecil”. Mikrotik berkantor pusat di Latvia, Produk-produk *hardware* yang merupakan produksi unggulan Mikrotik yaitu, *router*, *switch*, antena, dan perangkat pendukung lainnya, sedangkan untuk produk *Software* unggulan Mikrotik adalah MikroTik RouterOS.[4]

2.3. Metode otentikasi pengguna (user)

Metode otentikasi pengguna (*user*) pada hotspot merupakan berbagai cara atau prosedur yang digunakan untuk memverifikasi identitas pengguna sebelum mereka diizinkan mengakses jaringan *hotspot*. Otentikasi pengguna pada jaringan wireless dilakukan dengan WPA2/PSK yang diperoleh dari *security default* yang ada pada perangkat, dalam melakukan pengamanan sederhana dengan memakai kunci WPA.[5]

Dengan metode autentikasi pengguna, diharapkan sistem keamanan jaringan *hotspot* dapat beroperasi secara efektif, memastikan bahwa hanya pengguna sah atau terdaftar.[6]

2.4. Hotspot

Hotspot adalah suatu koneksi jaringan *Wireless* yang tersedia dan siap pakai, dimana pengguna dengan perangkat *WLAN* yang *compatible*, dapat terhubung ke internet atau *private* internet, *hotspot*

atau yang lebih dikenal sebagai *Wi-Fi hotspot* tersusun atas perangkat atau komponen *WLAN*, *server* dan *ISP* bila terhubung ke internet.[7]

Pengertian lain dari *Hotspot* adalah area di mana seorang klien dapat terhubung ke internet secara nirkabel atau tanpa kabel melalui PC, laptop, atau gadget seperti ponsel, dalam radius jangkauan sekitar beberapa ratus meter, tergantung pada kekuatan frekuensi atau sinyalnya.[8]

2.5. Winbox

Winbox adalah aplikasi yang dikembangkan oleh perusahaan Mikrotik untuk mengkonfigurasi dan mengelola perangkat jaringan berbasis RouterOS. Aplikasi ini umumnya digunakan oleh administrator jaringan dan pengelola sistem untuk mempermudah dan meningkatkan efisiensi dalam mengelola perangkat-perangkat Mikrotik.[9]

Perangkat lunak ini dirancang untuk memudahkan administrator dalam mengonfigurasi Mikrotik melalui antarmuka grafis (GUI), sehingga proses pembuatan jaringan komputer menjadi lebih sederhana.[10].

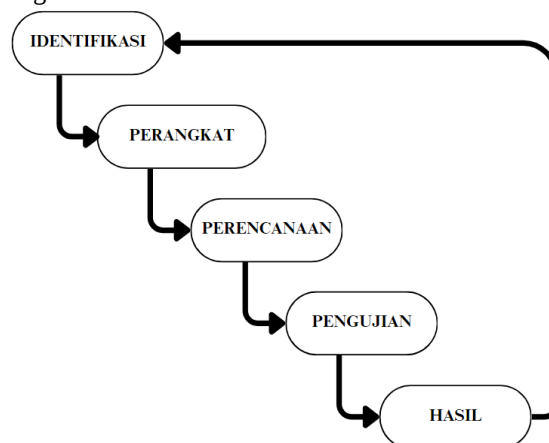
Semua fungsi Winbox dirancang dan dibuat sedemikian rupa agar mirip dan mendekati fungsi konsol. Dengan demikian, Anda akan menemukan istilah-istilah yang sama seperti yang ada pada fungsi konsol.[11]

2.6. One-Time Password(OTP)

One-time password (OTP) adalah kata sandi atau kode verifikasi yang hanya berlaku untuk satu kali login atau transaksi (Kalaikavitha & Gnanaselvi, 2013). OTP digunakan untuk mengatasi beberapa kelemahan yang terkait dengan kata sandi statis. Tidak seperti kata sandi statis, OTP tidak rentan terhadap serangan replay. Oleh karena itu, meskipun penyusup berhasil merekam OTP, mereka tidak dapat menggunakannya karena OTP tersebut sudah tidak berlaku lagi.[1]

3. METODE PENELITIAN

Peneliti menggunakan metode “Otentikasi Pengguna (*user*)” dengan Menggunakan *One-Time Password(OTP)* supaya bisa membagi prioritas jaringan untuk pengguna sah sehingga tidak adanya pengguna asing.



Gambar 1. Framework Penelitian

3.1. Identifikasi

Identifikasi dilakukan untuk mengetahui penyebab masalah dan mencari solusi yang tepat untuk menyelesaikan permasalahan tersebut. Langkah awal yang akan dilakukan pada penelitian ini adalah melakukan observasi lapangan, melakukan analisis masalah, dan yang terakhir yaitu menentukan metode penelitian yang digunakan.

3.2. Analisis masalah yang terjadi

Berdasarkan observasi lapangan yang dilakukan peneliti, diperoleh hasil bahwa saat jaringan *hotspot* diakses oleh banyak pengguna, kecepatan internet saat melakukan *download*, *upload* dan *browsing* menjadi kurang baik di beberapa perangkat. Hal ini dikarenakan banyaknya user pengguna asing yang mengakses internet sepatutnya diimbangi dengan jaminan kerahasiaan data dari orang-orang yang tidak berkepentingan.

3.3. Menentukan metode penelitian

Dari analisis masalah diatas, maka diperlukan sebuah manajemen *keamanan* yang baik, agar kecepatan jaringan bisa stabil. Begitu juga dengan tidak adanya pembagian kelompok *user* pengguna *hotspot*. Maka perlu dilakukan perancangan sebuah proses autentikasi, peneliti menggunakan metode “Otentikasi Pengguna (*user*)” dengan Menggunakan *One-Time Password(OTP)* supaya bisa membagi prioritas jaringan untuk pengguna sah sehingga tidak adanya pengguna asing.

3.4. Perangkat keras

Merupakan perangkat yang dapat digerakkan atau fisik. Berikut ini adalah beberapa contoh perangkat keras yang digunakan untuk membangun jaringan *hotspot* dan sistem keamanannya :

Tabel 1. Hardware

No	Hardware	Type
1	Mikrotik	RB 951 Ui 2HnD
2	PC/LAPTOP	Thinkpad T14S
3	Kabel LAN	Cat 6
4	Wireless Modem	ZTE

3.5. Perangkat lunak

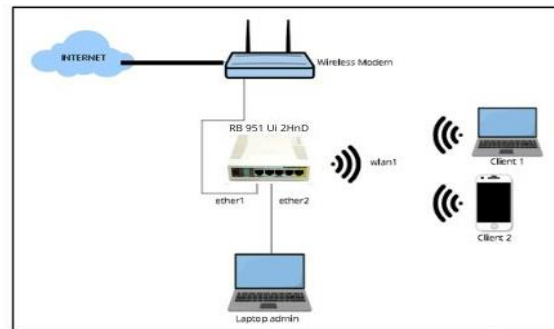
Atau juga biasa disebut *software*, adalah aplikasi atau alat yang dapat dijalankan pada laptop atau komputer. Pada rancangan penelitian ini, peneliti menggunakan beberapa perangkat lunak, sebagai berikut:

Tabel 2. Software

No	Software	Type
1	Windows	Windows 11
2	Winbox	Versi 3.40
3	Mikrotik Router OS	Versi 7.15.1

3.5. Perencanaan

Menerapkan metode “Otentikasi Pengguna (*user*)”. Gambar 3.2 menunjukkan bahwa topologi jaringan masih menggunakan topologi yang sedang berjalan namun hanya menambahkan *router*.



Gambar 2. Topologi yang digunakan

Berikut merupakan rancangan IP baru yang peneliti tentukan untuk membantu dan menyelesaikan penelitian ini, IP tersebut akan dikonfigurasi pada perangkat *router* mikrotik.

Tabel 3. Rancangan IP

No	Interface	Ip
1	Ether 1	192.168.74.0/24
2	Ether 2	10.5.50.1/24

Setelah sudah membuat IP dan topologi baru yang sesuai dengan kebutuhan, selanjutnya masuk tahap konfigurasi. Pada tahap ini peneliti melakukan konfigurasi pada kelompok *user*, konfigurasi tersebut dilakukan pada aplikasi winbox.

3.6. Pengujian

Tahap pengujian pada konfigurasi jaringan *hotspot* Mikrotik ini melibatkan beberapa langkah yang bertujuan untuk memastikan bahwa jaringan yang dibangun berfungsi sesuai dengan tujuan yang diinginkan. Berikut adalah beberapa tahap pengujian yang umum dilakukan :

3.6.1. Pengujian Generate Authenticator Pertama

Yaitu pengujian *Generate One-Time Password(OTP)* pada setiap kelompok *user*, apakah sudah memasang Extension Google Authenticator pada website sehingga pengguna akan diberikan kode Otp secara acak yang akan digunakan untuk login ke jaringan *Hotspot*.

3.6.2. Login

Tahap Selanjutnya, metode otentikasi pengguna (*user*) diuji dengan cara melakukan login ke masing-masing akun pengguna sesuai dengan *user* dan *password* yang tersedia yang diberikan secara OTP dari Google Authenticator dan untuk memastikan bahwa hanya pengguna yang berhasil melakukan otentikasi yang bisa mengakses jaringan internet.

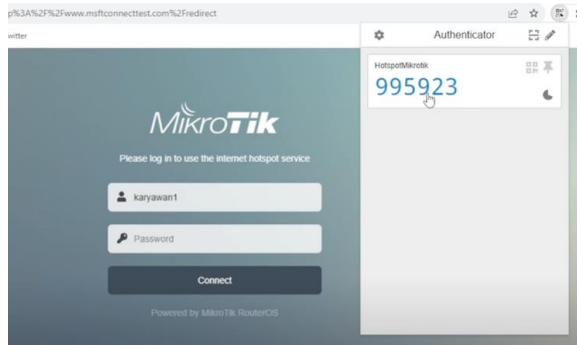
4. HASIL DAN PEMBAHASAN

Adapun hasil penelitian dari perancangan jaringan *hotspot* berbasis mikrotik RB951-2HnD dengan metode otentikasi pengguna (*user*) menggunakan *One-time Password(OTP)* ini adalah sebagai berikut :

- Dapat merancang jaringan *hotspot* yang mampu memberikan koneksi yang lebih stabil serta meningkatkan keamanan jaringan *hotspot* sehingga membantu efisiensi kerja pengguna.
- Dapat menerapkan metode otentikasi pengguna (*user*) dengan menggunakan *One-time password(OTP)* untuk keamanan manajemen jaringan.

Tahap pengujian, di tahap ini peneliti melakukan pengujian login ke user yang sudah di buat, pengujian dilakukan di *Virtual Box* yang sudah terinstall system operasi windows 11.

- Masuk ke halaman login *hotspot* mikrotik, kemudian kita lakukan proses generate kode OTP menggunakan ekstensi “*Authenticator*”



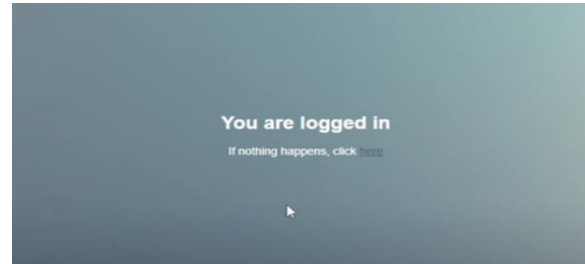
Gambar 3. Kode Generate Authenticator

- Masukan *username* sesuai dengan yang sudah kita konfigurasi di menu *user manager* dan untuk *password*, isi sesuai dengan kode OTP yang sudah di generate.



Gambar 4 Tampilan Login

- Setelah *username* dan *password* input, maka *user* sudah berhasil login dan bisa mengakses jaringan *hotspot* yang disediakan.



Gambar 5 Tampilan Terhubung ke jaringan

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan maka didapatkan kesimpulan, yaitu perancangan keamanan jaringan *hotspot* pada UP-TIK UM Bengkulu berhasil dan telah sesuai dengan kebutuhan penggunaan internet untuk kegiatan *download*, *upload* dan *browsing*. Selain itu perancangan metode otentikasi pengguna (*user*) menggunakan *One-time Password(OTP)* ini didapatkan hasil bahwa lebih aman. Sehingga jaringan *hotspot* akan menjadi lebih stabil dalam menangani beberapa pengguna asing yang Mengakses Hotspot. Adapun saran-saran yang dapat penulis sampaikan berdasarkan hasil yang diperoleh dari penelitian ini adalah: Bagi peneliti yang ingin melanjutkan penelitian ini, diharapkan untuk menambah satu perangkat access point yang terhubung langsung ke mikrotik, supaya sistem *hotspot* bisa bekerja dengan lebih baik lagi. Dan bagi peneliti selanjutnya, diharapkan bisa mengatasi masalah pada radius server, dimana pada penelitian ini, sering terjadi radius server tidak merespon atau Radius server *not responding* sehingga tidak bisa terkoneksi ke *hotspot*.

DAFTAR PUSTAKA

- [1] M. A. Taqwim, A. Kusyanti, and R. A. Siregar, “(OTP)Implementasi Algoritme Speck Untuk Enkripsi One-Time Password Pada Two-Factor Authentication,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 7, pp. 3103–3111, 2021, [Online]. Available: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/9488>
- [2] O. H. Kelana, P. L. T. Irawan, and P. M. Halim, “(OTP)Implementasi One Time Password dengan Metode Advanced Encryption Standard,” *Pros. Semin. Nas. Univ. Ma Chung*, vol. 1, pp. 81–90, 2021, doi: 10.33479/snumc.v1i.233.
- [3] Azhar, Arkarni Wais, and Atthariq, “(OTP)Sistem Keamanan Pada Halaman Login Menggunakan One Time Password,” *J. Embed. Syst. Secur. Intell. Syst.*, vol. 01, no. 2, pp. 106–113, 2020.
- [4] I Kadek Juni Arta and Nyoman Bagus Suweta Nugraha, “Implementasi Aplikasi User Management Hotspot Mikrotik Berbasis Php Dengan Application Programming Interface (Api) Dan Framework Bootstrap,” *J. Resist. (Rekayasa Sist. Komputer)*, vol. 3, no. 1, pp. 66–71, 2020, doi: 10.31598/jurnalresistor.v3i1.466.
- [5] M. Rayza *et al.*, “Keamanan Jaringan Hotspot Mikrotik Menggunakan Metode Otentikasi Pengguna dengan Captcha dan IP-Binding Untuk

- Filtering User,” no. September, pp. 322–331, 2023.
- [6] F. Ardianto, B. Alfaresi, and R. A. Yuansyah, “Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Otentikasi Pengguna,” *J. Surya Energy*, vol. 2, no. 2, p. 167, 2018.
- [7] J. F. Fitrian and H. Sujadi, “Implementasi Hotspot Dengan Pengelolaan User Manager Dan Bandwidth Menggunakan Mikrotik Rb941-2Nd (Studi Kasus Smk Kesehatan Bhakti Kencana Jatiwangi),” *Pros. Semin. Nas. Penelit. dan Pengabd. Kpd. Masy.*, vol. 1, no. 1, pp. 103–110, 2023.
- [8] H. S. Syahputra and R. WIjaya, “Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara,” *Maj. Ilm. UPI YPTK*, vol. 29, no. 1, pp. 60–66, 2022, doi: 10.35134/jmi.v29i1.108.
- [9] M. Arrahman, A. Yulio Pernanda, and R. Novita, “Pengembangan Sistem Manajemen Bandwidth Dengan Metode Hierarchical Token Bucket Di Smkn 9 Padang,” *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 7, no. 4, pp. 2673–2682, 2024, doi: 10.36040/jati.v7i4.7528.
- [10] D. Bahtiar *et al.*, “Pengenalan Dasar Instalasi Jaringan Komputer Menggunakan Mikrotik,” *Kreat. Mhs. Inform.*, vol. 2, pp. 507–518, 2021, [Online]. Available: <https://core.ac.uk/download/pdf/524980292.pdf>
- [11] S. Dwiyatno, Sulistiyono, E. Rakhmat, and S. Christina, “Perancangan Private Cloud Berbasis Infrastructure As a Service,” *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 8, no. 2, pp. 5–14, 2021, doi: 10.30656/prosisko.v8i2.3705.