

Implementasi The Onion Router (Tor) Berbasis Virtual Private Network (VPN) pada Raspberry Pi

Kenny¹, Kartika Gunadi², Leo Willyanto Santoso³

Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Kristen Petra

Jl. Siwalankerto 121 – 131 Surabaya 60236

Telp. (031) – 2983455, Fax. (031) – 8417658

E-mail: m26413080@john.petra.ac.id, kgunadi@petra.ac.id, leow@petra.ac.id

ABSTRAK

Internet yang kita gunakan sehari - hari tidak sepenuhnya aman dari *hackers* yang akan melakukan *cybercrime*. Saat ini, Internet telah menjadi bagian dari kehidupan kita sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk perorangan. Tetapi di balik itu masih banyak lubang kelemahan sistem di internet yang bisa dimanfaatkan oleh para hacker untuk tujuan tidak baik, seperti mail bomb, pengacak-acakan homepage, pencurian data, password ataupun nomor kartu kredit. Keamanan yang sering digunakan orang pada umumnya hanya sistem keamanan yang mendasar saja.

Aplikasi ini dibuat dengan menggunakan bahasa pemrograman Python dan html. Tampilan aplikasi menggunakan Bottle Python Web Framework yang dapat diakses melalui ip gateway. Aplikasi ini dibuat dalam Raspberry Pi yang dilengkapi dengan LCD 16x2.

Hasil akhir dari pengembangan aplikasi ini adalah dapat menggunakan VPN dan Tor secara bersamaan sehingga surfing/browsing pada internet menjadi lebih aman dan dapat mengakses beberapa website yang telah terblokir seperti forum reddit. Dengan aplikasi ini cyber hacker akan mengalami kesusahan dalam melakukan tracking.

Kata Kunci: Raspberry Pi, VPN, Tor, Python, BottlePy.

ABSTRACT

Internet that we use everyday is not fully secured from hackers that want to do cybercrime. Today, the Internet has become part of our daily lives as one of the means of communication in business as well as for individuals. But behind that there are many holes weakness of the system on the internet that can be exploited by the cracker for not good purposes, such as mail bombs, randomization of home page, data theft, password or credit card number. Most of security that people used in general is only the basic security system.

This application is created using the programming language Python and html. The interface of app using Bottle Python Web Framework that can be accessed via IP Gateway. This is made in Raspberry Pi which is equipped with 16x2 LCD.

The result of this development is we are able to use VPN and Tor simultaneously so that surfing / browsing on the internet becomes more secure and can access some websites that have been blocked like reddit forum. With this application cyber hackers will have trouble in doing tracking.

Keywords: Raspberry Pi, VPN, Tor, Python, BottlePy.

1. PENDAHULUAN

Internet menjadi salah satu kebutuhan pokok saat ini. Manfaat internet adalah menghubungkan jaringan yang tidak saling bergantung pada satu sama lain sedemikian rupa, sehingga dapat berkomunikasi dan bekerja secara baik dan tanpa masalah. Internet dapat bekerja dalam sistem apa pun, seperti Windows, DOS, atau Linux sekalipun. Kebutuhan akan informasi yang up to date menjadi faktor yang mewajibkan setiap individu untuk terkoneksi ke jaringan internet. Namun keindahan Internet tidak seindah namanya yang dijanjikan dapat memberikan berbagai informasi yang ada di belahan dunia mana pun, karena berbagai kejahatan yang ada di kehidupan nyata ternyata lebih banyak ditemukan di dunia Internet.

Internet yang kita gunakan sehari - hari tidak sepenuhnya aman dari *hackers* yang melakukan *cybercrime*. Saat ini, Internet telah menjadi bagian dari kehidupan kita sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk perorangan. Tetapi di balik itu masih banyak lubang kelemahan sistem di internet yang bisa dimanfaatkan oleh para cracker untuk tujuan tidak baik, seperti mail bomb, pengacak-acakan home page, pencurian data, password ataupun nomor kartu kredit. Keamanan yang sering digunakan orang pada umumnya hanya sistem keamanan yang mendasar saja. Seperti Windows Firewall, port block pada router, dan privasi dari provider internet. Virtual Private Network (VPN) dapat memperkuat keamanan pada user dengan bantuan program pihak ketiga pada sistem operasi Windows seperti OpenVPN dan server VPN seperti vpngate.net. The Onion Router (Tor) juga dapat memperkuat keamanan user dengan sistem keamanan yang lebih kuat daripada VPN saat melakukan surfing di internet. Tor pada sistem operasi Windows menggunakan program pihak ketiga yaitu Tor Browser. Namun VPN dan Tor pada Windows lebih rumit dalam berganti-ganti koneksi.

Oleh karena itu, dengan membuat router access point berbasis Raspberry Pi sistem keamanan dapat ditambah dengan WPA2, VPN, dan Tor. Penulis mencoba memanfaatkan teknologi hostapd yang membuat Raspberry Pi menjadi router access point atau hotspot dan menggunakan koneksi VPN dan Tor agar koneksi ke website menjadi anonymous sehingga user tidak perlu khawatir ketika surfing ke website.

2. TINJAUAN PUSTAKA

2.1 Raspberry Pi

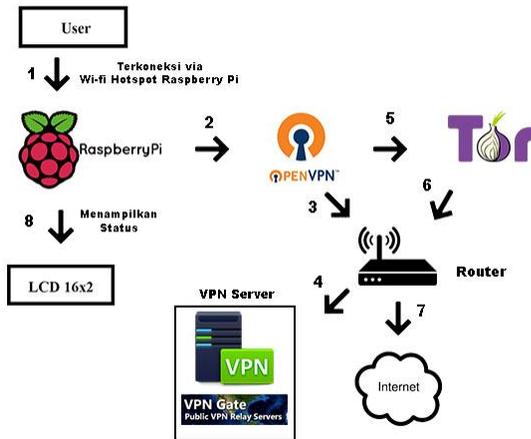
Raspberry Pi adalah komputer yang memiliki sistem operasi Linux. Komputer ini, memiliki soket USB yang dapat dipakai untuk keyboard dan mouse. Raspberry Pi menggunakan kartu SD

sebagai pengganti hard disk yang berguna untuk menyimpan sistem operasi. Saat booting, terdapat Linux desktop yang lengkap dengan office suite, pemutar video, games, dan lain-lain. Dalam penjualannya, Raspberry Pi hanya sebuah board tanpa case yang melindunginya.[3]

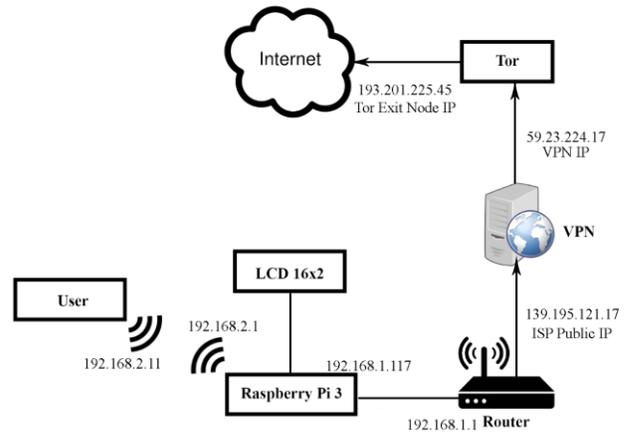
Di dalam Raspberry Pi ini, terdapat GPIO (general purpose input/output) pins yang membuat Raspberry Pi dapat terhubung dengan custom electronics. Terdapat juga Wi-Fi serta Bluetooth yang sudah terintegrasi saat membeli unit ini. Raspberry Pi 3 dapat dilihat pada Gambar 1 sedangkan sistem operasinya dapat dilihat pada Gambar 2.



Gambar 1. Rasberry Pi 3



Gambar 2. Desain Cara Kerja Perangkat



Gambar 3. Desain Cara Kerja Program

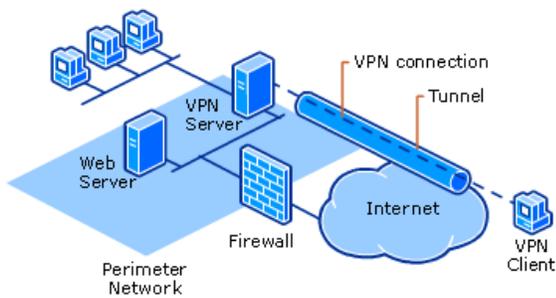
2.2 Hostapd

Hostapd adalah user space daemon untuk access point dan autentikasi server. Hostapd mempunyai implementasi IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/EAP Authenticators, RADIUS client, EAP server, and RADIUS authentication server. Versi terbaru dari Hostapd dapat dijalankan pada sistem operasi Linux (Host AP, madwifi, mac80211-based drivers) dan FreeBSD (net80211). Hostapd dibuat untuk menjadi program “daemon” yang beroperasi di balik layar dan berperan sebagai backend component controlling authentication. Hostapd dapat dijalankan pada program frontend dan contoh frontend yang bersifat text-based seperti hostapd_cli yang terdapat pada hostapd.[4]

2.3 VPN

VPN adalah teknologi yang memungkinkan kita mengakses internet jika kita tersambung dari lokasi-lokasi berbeda. Ini berarti, di antaranya operator ISP/jaringan lokal kita tidak dapat memeriksa atau memfilter trafik dan setiap situs atau layanan lainnya akan melihat alamat IP kita yang berbeda-beda.[6]

VPN singkatan dari "Virtual Private Network". Istilah ini mengacu kepada seperangkat teknologi yang memungkinkan komputer untuk terhubung ke jaringan pribadi melalui internet (atau jaringan publik lainnya), dan bertukar data dengan komputer lainnya di dalam jaringan aman seolah-olah secara fisik merupakan bagian dari jaringan tersebut. Hal ini biasanya dicapai dengan membentuk koneksi terenkripsi dengan komputer jarak jauh dan "mengarahkan" semua trafik melalui koneksi tersebut. Meskipun VPN digunakan untuk berbagai tujuan, "layanan VPN" paling sering mengacu kepada penyedia konektivitas VPN yang digunakan untuk mengarahkan semua trafik internet agar melewati ISP lokal. Cara kerja VPN adalah user device akan terkoneksi ke internet kemudian akan terhubung dengan VPN server terlebih dahulu. Setelah terhubung dengan VPN server, koneksi akan terhubung dengan Web Server dengan IP Network dari VPN server. Gambar detail cara kerja VPN dapat dilihat pada Gambar 4.



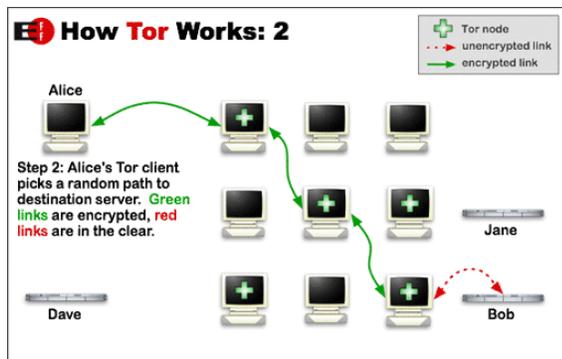
Gambar 4. Contoh cara Kerja VPN

2.4 Tor

Tor adalah akronim dari The Onion Router. Jaringan Tor adalah sekelompok relawan operasi server yang memungkinkan orang lain untuk meningkatkan privasi dan keamanan mereka ketika melakukan surfing di internet. Penggunaan Tor menggunakan jaringan ini dengan terhubung melalui serangkaian virtual tunnels dan tidak melalui koneksi langsung, sehingga memungkinkan kedua organisasi dan individu untuk berbagi informasi melalui jaringan publik tanpa mengorbankan privasi mereka.[5]

Kegunaan Tor yang lain adalah alat sensor pengelakan yang efektif dan memungkinkan penggunanya untuk mengakses website atau konten yang terblokir. Tor juga dapat digunakan sebagai sebuah building block dalam pengembangan perangkat lunak untuk menciptakan alat komunikasi baru dengan built-in fitur privasi. [4]

Onion Routing (OR) memiliki kemampuan yang sama dengan VPN yaitu dapat menyembunyikan Internet Protocol (IP) milik user yang sebenarnya. Namun Tor mengirim paket dari satu node ke node lainnya hingga dapat mencapai responder atau website yang dituju. Operasi dari Onion Routing terjadi dalam 4 tahap, yaitu Network Setup, Connection Setup, Data Movement, dan Connection Destruction. Data yang dikirim dari tahap pertama hingga tahap terakhir sudah dijadikan menjadi anonymous atau tidak diketahui. Data yang akan diterima menggunakan 4 tahap yang sama tetapi dari node terakhir pada proses tersebut. [1]

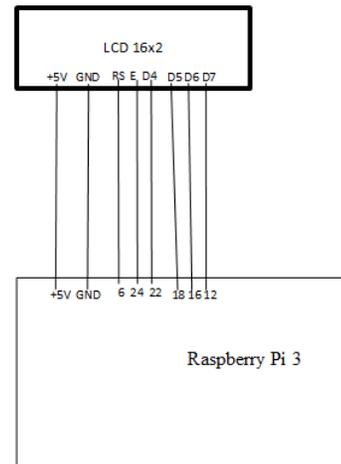


Gambar 5. Contoh cara Kerja Tor

3. ANALISA DAN DESAIN SISTEM

3.1 Desain Perangkat Keras

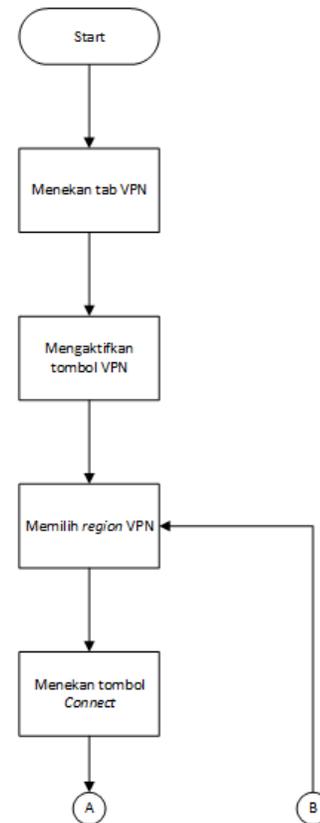
Perangkat keras yang digunakan pada program ini adalah Raspberry Pi 3 dan LCD 16x2 Keypad Shield seperti pada Gambar 3.1. Raspberry Pi 3 dan LCD berinteraksi melalui GPIO yang sudah terkoneksi dengan menggunakan kabel jumper. Desain Perangkat Keras dapat dilihat pada Gambar 6.



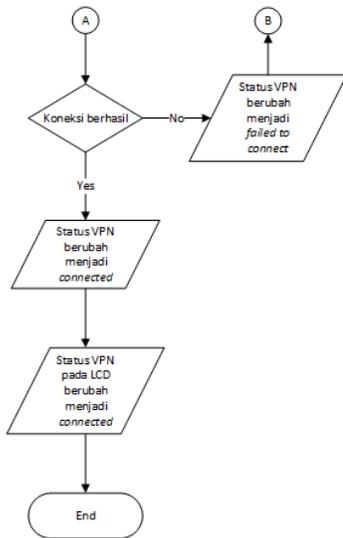
Gambar 6. Desain Perangkat Keras

3.2 Flowchart VPN

Proses VPN dilakukan dengan menekan tab VPN, kemudian mengaktifkan tombol VPN dengan memilih enable pada radio button. User dapat memilih region yang akan digunakan lalu menekan tombol Connect. Jika koneksi berhasil maka status VPN akan berubah menjadi connected, sedangkan jika koneksi gagal, maka status VPN akan berubah menjadi failed to connect dan user akan diarahkan untuk memilih region VPN lain. Status VPN pada LCD juga akan berubah sama dengan status yang tertera pada web panel. Desain flowchart dapat dilihat pada Gambar 7.



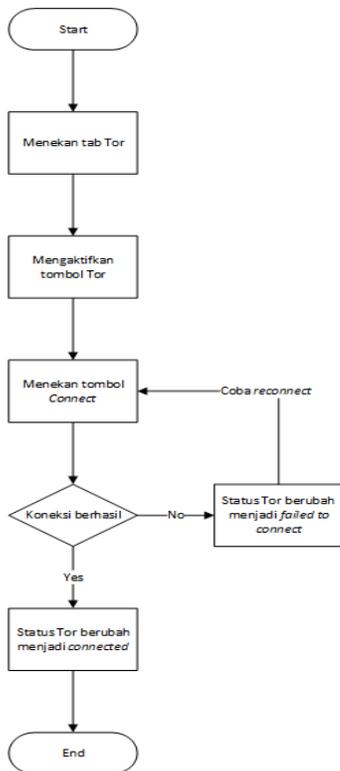
Gambar 7. Desain flowchart VPN



Gambar 8. Desain flowchart VPN (lanjutan)

3.3 Flowchart Tor

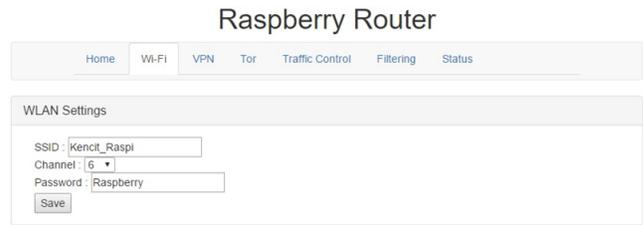
Proses Tor dilakukan dengan menekan tab Tor, kemudian mengaktifkan tombol Tor dengan memilih enable pada radio button. User menekan tombol Connect. Jika koneksi berhasil maka status Tor akan berubah menjadi connected, sedangkan jika koneksi gagal, maka status Tor akan berubah menjadi failed to connect dan user akan diarahkan untuk mencoba menekan tombol Connect lagi. Status Tor pada LCD juga akan berubah sama dengan status yang tertera pada web panel. Desain flowchart dapat dilihat pada Gambar 7.



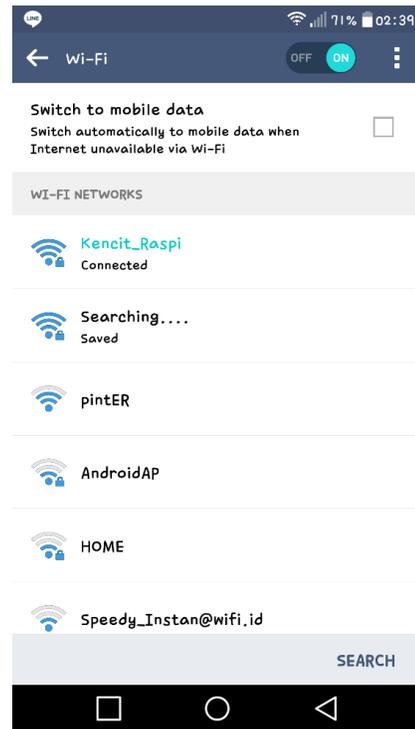
Gambar 9. Desain flowchart Tor

4. HASIL

Hasil aplikasi berupa aplikasi web dan LCD. Gambaran aplikasi secara umum seperti pada Gambar 9 dan Gambar 10.



Gambar 9. Tampilan Aplikasi



Gambar 10. Tampilan Wi-fi



Gambar 11. Tampilan LCD

Halaman VPN digunakan untuk menyalakan dan mematikan VPN. User juga dapat memilih region VPN yang akan digunakan. Tampilan menu vpn dapat dilihat pada Gambar 12.



Gambar 12. Tampilan Menu VPN



Gambar 13. Tampilan koneksi VPN

Halaman Tor digunakan untuk menyalakan dan mematikan Tor. Tampilan menu tor dapat dilihat pada Gambar 14.



Gambar 14. Tampilan Menu Tor



Gambar 15. Tampilan koneksi Tor

5. KESIMPULAN

Dari hasil pembuatan router access point dengan VPN yang berbasis Tor, dapat diambil kesimpulan antara lain:

- Koneksi Tor menjadi lebih aman karena telah tertutup oleh IP dari VPN sehingga tidak mudah di deteksi oleh website – website yang dapat melakukan pelacakan pada pengunjung website.
- Dengan access point menggunakan Raspberry Pi, user dapat melakukan limitasi bandwidth secara merata untuk tiap usernya.

6. DAFTAR PUSTAKA

- [1] AlQahtani, A.A. & El-Alfy, E.A. 2015. Anonymous connections based on onion routing: A review and a visualization tool.
- [2] Horan, B. 2013. Practical Raspberry Pi. New York: Business Media New York
- [3] Malinen, J. 2016. hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator. Retrieved November 20, 2016, from <http://w1.fi/hostapd/>
- [4] Torproject.org (n.d.) Tor Overview. Retrieved November 20, 2016, from <https://www.torproject.org/about/overview.html.en>
- [5] Wang, C., Shi, D. & Xu, X. 2015. AIB-OR: Improving Onion Routing Circuit Construction Using Anonymous Identity-Based Cryptosystems. PLoS ONE 10(3): e0121226. doi:10.1371/journal.pone.0121226
- [6] Zenvpn.net. 2013. Apa itu VPN?. Retrieved July 10, 2017, from <https://zenvpn.net/id/what-is-vpn/>