



Implementation Of Secure Detection And Monitoring For Intelligence's Target (SDMIT)

Indrian Alfiansyah¹

¹ Akademi Angkatan Udara, Yogyakarta, Indonesia

e-mail : indrian22@gmail.com

Abstrak—Operasi intelijen merupakan kegiatan pengumpulan informasi penting maupun yang berguna bagi pihak sendiri untuk kepentingan pertimbangan pengambilan keputusan oleh pimpinan. Operasi intelijen dapat disebut *clandestine*, kegiatan operasi intelijen dapat berupa penyelidikan, pengamanan, dan penggalangan. Penelitian ini akan membahas mengenai implementasi alat pendeteksi dan *monitoring* target intelijen yang akan berguna untuk intelijen dalam membantu menyelesaikan tugas pokok yang diberikan dalam penyelidikan dan pengamanan. Hasil implementasi tersebut diwujudkan dalam suatu alat yaitu *Secure Detection and Monitoring for Intelligence's Target*. Alat ini terdiri dari tiga bagian besar, bagian pertama terdiri dari bagian sensor gerak *PIR* dan *NodeMCU* yang berguna untuk mendeteksi target dan mengirimkan sinyal ke bagian yang kedua. Bagian kedua terdiri dari motor *Servo* dan *Raspberry pi Zero W* dan Kamera kecil yang akan aktif ketika mendapat sinyal dari bagian pertama. Kamera akan terus memonitor target dengan digerakan berputar 180 derajat kekanan dan kekiri. Data *video streaming* akan dikirimkan ke bagian ketiga yaitu komputer atau *handphone* kita. Jalur komunikasi *Streaming video* diamankan dengan teknik persandian yaitu dengan implementasi *OpenVPN Server* pada *Raspberry pi Zero W*, dan data sinyal yang dikirimkan dari *nodeMCU* ke *Raspbaryy pi Zero W* diamankan melalui implementasi protokol *MQTT*. Semua lalu lintas data telah diamankan dengan teknik persandian dan semua perangkat yang digunakan berukuran kecil dan disamarkan. Implementasi *Secure Detection and Monitoring for Intelligence's Target* dapat membantu intelijen dalam melaksanakan dan menyelesaikan tugas operasi yang dilakukan melalui *monitoring* aktivitas target dari jarak jauh secara aman, melalui pengamanan data yang ditransmisikan. Semua hal yang dilakukan diharapkan bisa membantu dalam menyelesaikan tugas pokok intelijen yang diberikan.

Kata Kunci— *Camera Monitoring, Intelijen, MQTT, NodeMCU, PIR, Raspberry pi Zero W, OpenVPN, Wifi*

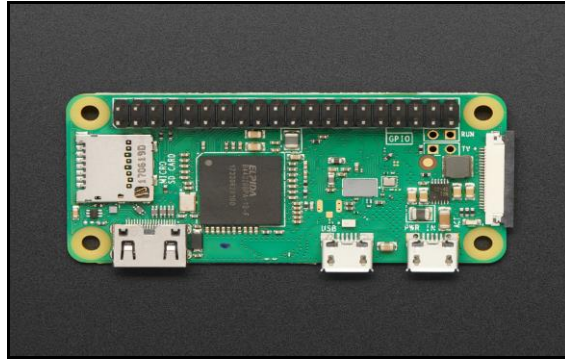
I. PENDAHULUAN

Pada penelitian ini akan dibahas mengenai pembuatan suatu alat yang bisa digunakan oleh seorang intelijen dalam melaksanakan tugas pokok yang diberikan. Alat tersebut diimplementasikan untuk bisa memonitor kegiatan target. Kegiatan *monitoring* tersebut dilakukan dengan mengirimkan *video streaming* secara *real time* melalui jaringan *wifi* yang sudah diamankan datanya melalui implemementasi *OpenVPN Server* pada *Raspbaryy pi Zero W*. Alat teraebut bekerja dengan memiliki tiga bagian atau komponen utama. Bagian pertam terdiri dari sensor *PIR* yang akan mendeteksi adanya gerakan dari target dan *nodeMCU* yang berguna mengirimkan data sensor ke *Raspberry pi Zero W* melalui *wifi*. Bagian kedua terdiri dari motor *Servo* yang berfungsi menggerakkan kamera 180 derajat kekanan atau kekiri sesuai kendali pengguna dan *Raspberry pi Zero W* yang berfungsi sebagai mikroprosesor yang menerima data dari *nodeMCu*, mengolah data *streaming video*, dan sebagai *OpenVPN server*. Kemudian bagian ketiga terdiri dari komputer atau *handphone* yang terkoneksi dengan jaringan *wifi* yang sama dengan *Raspberry pi Zero W* dan *NodeMCU*. Bagian ketiga berfungsi sebagai klien *openVPN*, membangun koneksi aman ke *OpenVPN server*, mengendalikan motor *Servo* dan menampilkan data *streaming video* kepada pengguna. Selain iti juga diimplementasikan protokol *MQTT* untuk menghubungkan sensor dengan *NodeMCU* sehingga data sensor yang dikirimkan aman. Selain itu semua alat diimplementasikan sekecil mungkin, disamarkan, dan menggunakan media nirkabel untuk mengelabui target. Diharapkana tersebut bisa membantu penyelesaian tugas operasi intelijen yang diberikan.

II. LANDASAN TEORI

Media komunikasi pengiriman data yang digunakan untuk mengirimkan data sensor dan data *video streaming* dapat menggunakan media wifi. Penggunaan wifi sebagai media pengiriman data karena wifi tidak memerlukan perangkat keras seperti kabel ketika digunakan menyalurkan data. Sifat ini sangat berguna untuk menghindari kecurigaan dari target intelijen yang sedang diintai. Semua alat didesain sekecil mungkin dan disamarkan sebaik mungkin agar target intelijen tidak curiga sedang dimata matai.

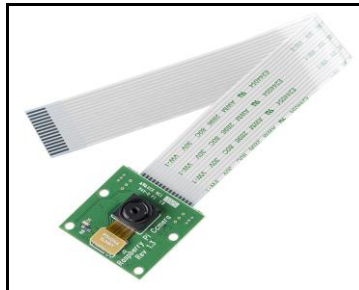
A. Raspberry pi Zero W



Gambar 1 *Raspberry pi Zero W* [1]

Pada Gambar 1 merupakan Gambar Microprosesor *Raspberry pi Zero W* yang berfungsi sebagai *OpenVPN server* dan mengendalikan proses *streaming video* yang dilakukan. Selain itu *Raspberry pi Zero W* berfungsi untuk mengendalikan *servo* untuk mengarahkan kamera sesuai arah yang diinginkan pengguna.

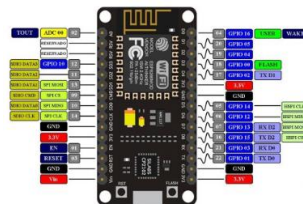
B. Camera Rev 1.3



Gambar 2 *Camera Rev 1.3* [2]

Pada Gambar 2 merupakan kamera Rev 1.3 yang berfungsi sebagai kamera yang merekam aktivitas target intelijen yang sedang dilakukan. Kamera ini akan aktif ketika *Raspberry pi Zero W* mendapat sinyal dari sensor gerak bahwa ada target yang bergerak.

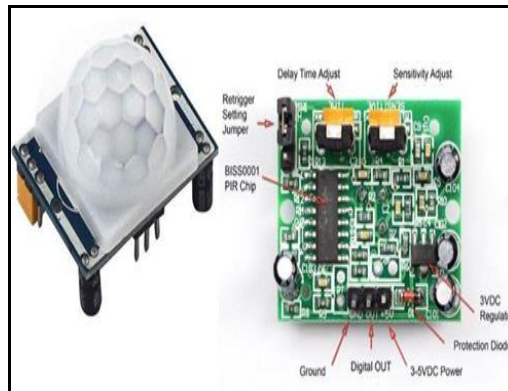
C. NodeMCU



Gambar 3 *NodeMCU* [3]

Pada Gambar 3 merupakan gambar *NodeMCU* merupakan suatu komponen mikrokontroler yang bisa terkoneksi dengan wifi. Komponen ini digunakan untuk mengendalikan sensor gerak *PIR* dan mengirim data sensor gerak *PIR* ke *Raspberry pi Zero W* melalui *wifi* jika terdapat pergerakan target.

D. PIR SENSOR



Gambar 4 *PIR Sensor* [4]

Pada Gambar 4 merupakan gambar *PIR sensor*. *PIR sensor* merupakan komponen berupa modul sensor untuk mendeteksi adanya gerakan dengan *infrared*. Komponen ini akan mendeteksi adanya gerakan target intelijen yang sedang diintai.

E. SERVO



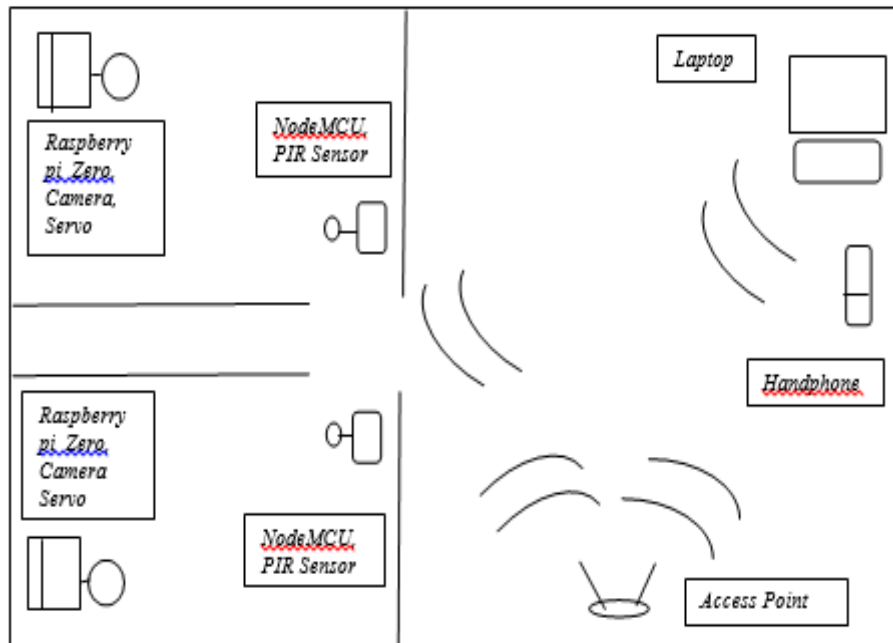
Gambar 5 *Servo* [5]

Pada Gambar 5 merupakan gambar *servo*. Pada penelitian ini *servo* berfungsi untuk menggerakkan kamera kekanan dan kekiri sejauh 180 derajat untuk membantu kaera dalam memonitoring aktivitas target intelijen.

III. MODEL YANG DIUSULKAN

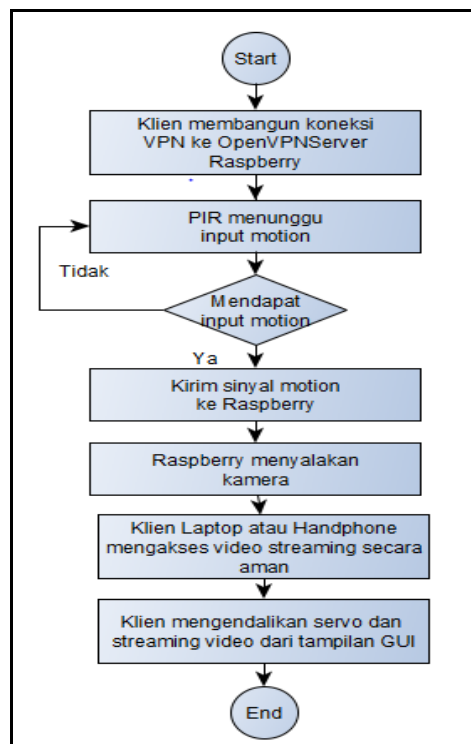
A. Arsitektur Model Secara Umum

Berikut adalah model secara umum dari system yang dibuat. Model sistem dibuat menjadi tiga bagian besar yang terpisah, bagian pertama yaitu *PIR Sensor* dan *NodeMCU* yang berfungsi mendeteksi dan mengirimkan sinyal gerakan ke bagian kedua. Bagian kedua terdiri dari *Raspberry* dan *Servo* yang berfungsi menerima sinyal dari bagian pertama dan *streaming video* dan mengirimkannya ke bagian ketiga. Bagian ketiga dari *Laptop* atau *Handphone* yagn berfungsi membangun koneksi *OpenVPN*, melihat *streaming video*, dan mengendalikan gerakan *Servo* untuk menggerakkan *Camera*. Berikut adalah mdel secara umum yang dibuat.



Gambar 6 Model sistem secara umum

B. Flowchart Sistem Implementasi SDMIT



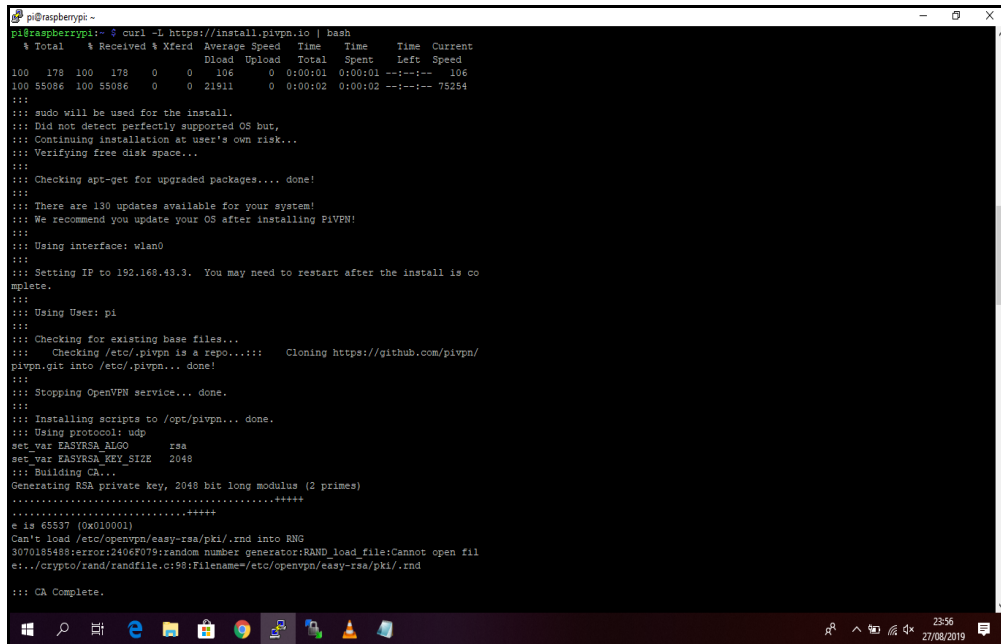
Gambar 7 Flowchart Implementasi Sistem

Pada Gambar 7 merupakan *flowchart* implementasi *Secure Detection and Monitoring for Intelligence's Target*. Hal pertama yang dilakukan adalah klien membangun koneksi *OpenVPN Server* ke *Raspberry pi Zero W* melalui *Handphone* atau *Laptop*. Setelah itu sensor *PIR* menunggu adanya input berupa gerakan. Jika mendapat sinyal gerakan maka akan diteruskan ke *NodeMCU* dan *NodeMCU* akan mengirimkan sinyal tersebut melalui *wifi* ke *Raspberry pi Zero W*. Setelah itu *Raspberry pi Zero W* akan menyalakan kamera dan mengirimkan *video streaming* ke klien. *Servo* berfungsi sebagai alat menggerakkan kamera kekanan atau kekiri sebesar 180 derajat.

IV. IMPLEMENTASI MODEL DAN PEMBAHASAN

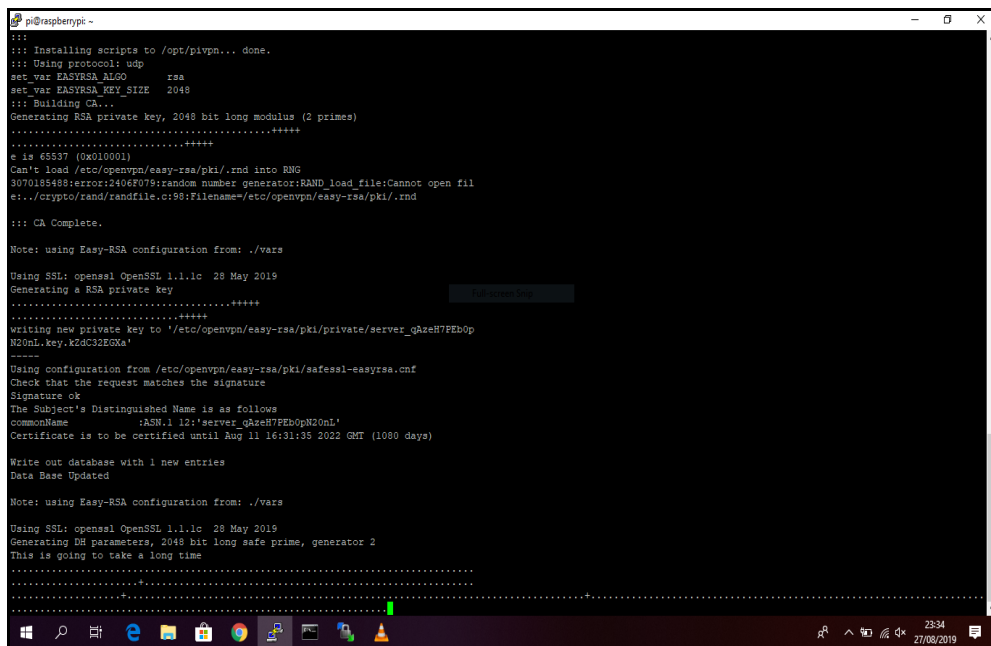
A. IMPLEMENTASI

Metodologi yang digunakan untuk merancang dan mengimplementasikan sistem menggunakan metodologi *waterfall development*. Berikut adalah gambar implementasi *OpenVPN Server* pada *Raspberry pi Zero W*. Pada Gambar 8 merupakan hasil implementasi *OpenVPN Server*, aplikasi yang ditanam pada *Raspberry pi Zero W* menggunakan *pipvn* yang sudah cocok untuk *Raspberry pi Zero W*.



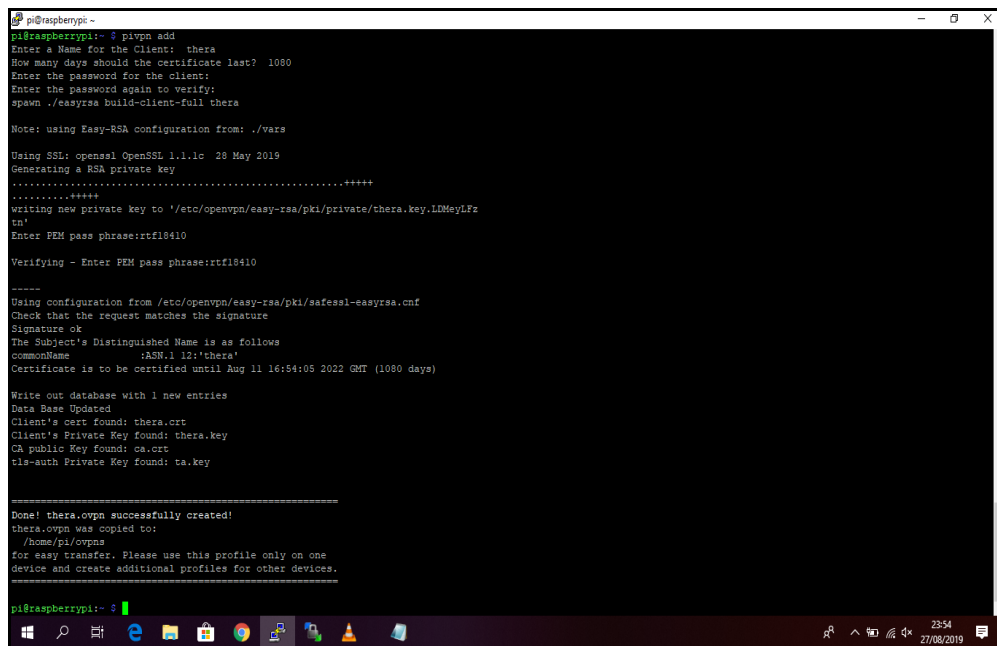
Gambar 8 Instalasi *OpenVPN Server*

Pada Gambar 9 merupakan hasil implementasi pembangkitan *Certificate Authority* pada *OpenVPN Server*. Sistem keamanan persandian yang digunakan menggunakan *RSA 2048 bit*. Sistem untuk merupakan standar untuk pengamanan data. Berikut hasil implementasi *Certificate Authority* pada *OpenVPN Server* yang dilakukan.



Gambar 9 Pembangkitan *Certificate Authority*

Pada Gambar 10 merupakan hasil implementasi untuk pendaftaran klien OpenVPN. Klien didaftarkan dengan nama dan kunci sandi untuk kunci *private* ditentukan oleh *admin*. Berikut hasil implementasi Pendaftaran Klien *OpenVPN*.



```

pi@raspberrypi:~$ ovpn add
Enter a Name for the Client: thera
How many days should the certificate last? 1080
Enter the password for the client:
Enter the password again to verify:
spawn ./easyrsa build-client-full thera

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 1.1.1c 28 May 2019
Generating a RSA private key
.....+++++
.....+++++
Writing new private key to '/etc/openvpn/easy-rsa/pki/private/thera.key.LDMeyLFz
tn'
Enter PEM pass phrase:rtf18410

Verifying - Enter PEM pass phrase:rtf18410

-----
Using configuration from /etc/openvpn/easy-rsa/pki/safessl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            : &#x1D; 12:'thera'
Certificate is to be certified until Aug 11 16:54:05 2022 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated
Client's cert found: thera.crt
Client's Private Key found: thera.key
CA public Key found: ca.crt
tls-auth Private Key found: ta.key

-----

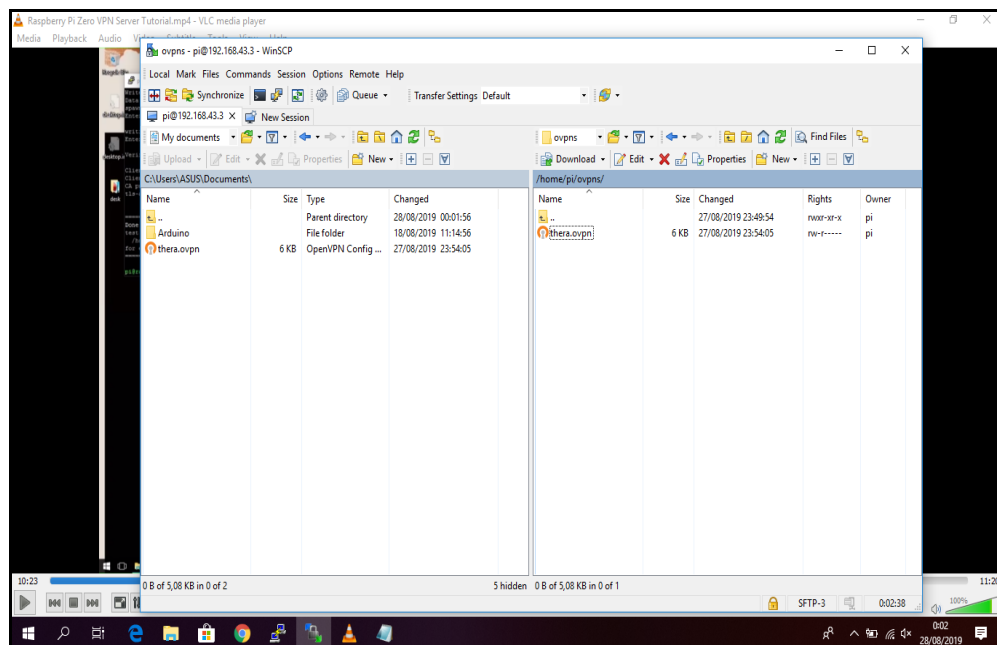
Done! thera.ovpn successfully created!
thera.ovpn was copied to:
/home/pi/ovpns
for easy transfer. Please use this profile only on one
device and create additional profiles for other devices.

pi@raspberrypi:~$

```

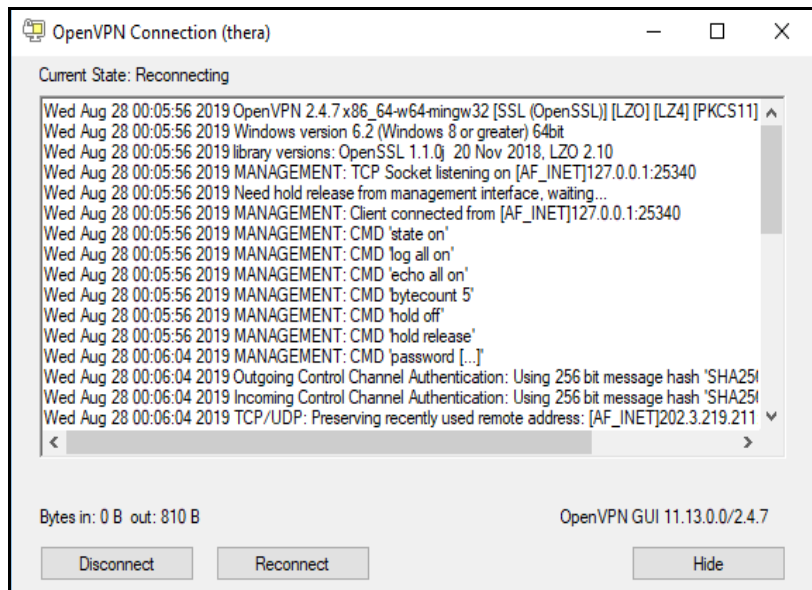
Gambar 10 Pendaftaran Klien *OpenVPN*

Pada Gambar 11 merupakan hasil implementasi untuk pemindahan file *ovpn* dari *server* ke klien. Pemindahan tersebut dilakukan dengan aplikasi *WinSCP* untuk *transfer file server*. *File ovpn* ini akan digunakan untuk konfigurasi pada klien *OpenVPN* di *laptop* atau di *handphone*. Berikut hasil implementasi pemindahan file *ovpn* dari *server* ke klien.



Gambar 11 Pemindahan *file ovpn* dari *server* ke klien

Pada Gambar 12 merupakan proses koneksi *OpenVPN* dari klien laptop ke *OpenVPN Server Raspberry pi Zero W*. Proses koneksi diawali dengan memasukkan kata sandi untuk kunci *private* yang digunakan. Berikut gambar proses koneksi *OpenVPN* klien ke *server*.



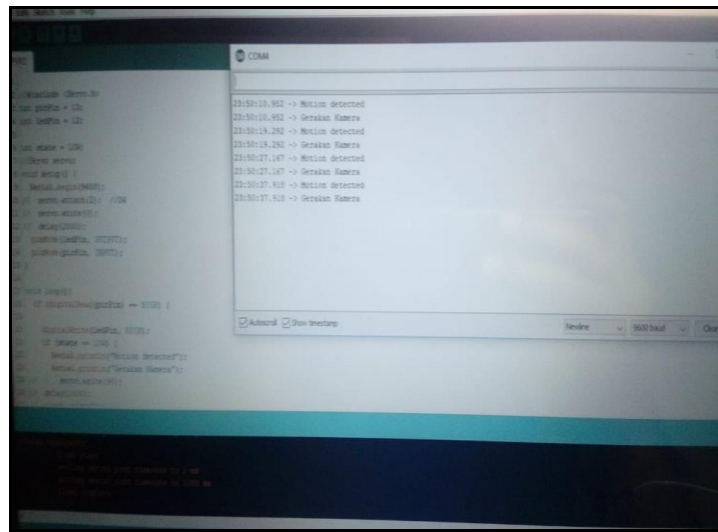
Gambar 12 Proses Memulai Koneksi *OpenVPN* dari *Laptop*

Pada Gambar 13 merupakan hasil implementasi untuk proses memulai koneksi dari klien *OpenVPN handphone* ke *server*. Proses ini diawali dengan memasukkan kunci sandi untuk kunci *privte* yang digunakan untuk memulai koneksi *OpenVPN*. Berikut hasil gambar proses memulai koneksi *OpenVPN* dari klien *handphone* ke *server*.



Gambar 13 Proses Memulai Koneksi *OpenVPN* dari *Handphone*

Pada Gambar 14 merupakan gambar hasil implementasi system untuk sensor pendeteksi gerakan. Sensor akan mengirimkan sinyal ke NodeMCU bahwa ada gerakan dan NodeMCU akan mengirimkan sinyal tersebut ke Raspberry pi Zero W untuk mengaktifkan kamera. Berikut hasil implementasi pendeteksi gerakan.



Gambar 14 Pendeteksi Gerakan

B. ANALISIS DAN PEMBAHASAN

Pada penelitian ini digunakan beberapa komponen perangkat keras dan beberapa aplikasi yang nantinya berguna dalam implementasi SDMIT. Alasan penggunaan modul ESP8266EX karena bisa terintegrasi dengan *Wifi*, mempunyai daya yang efisien, dan desain yang dapat diandalkan untuk internet of things pada industri serta ESP8266EX dapat berjalan sebagai modul wifi yang berdiri sendiri seperti MCU[3]. Kemudian untuk kamera yang digunakan oleh sistem yaitu menggunakan modul kamera versi 1.3 yang cocok dengan Raspberry pi Zero W dan mempunyai sensor gambar dengan 8 megapixel Sony IMX219 berkualitas tinggi[2].

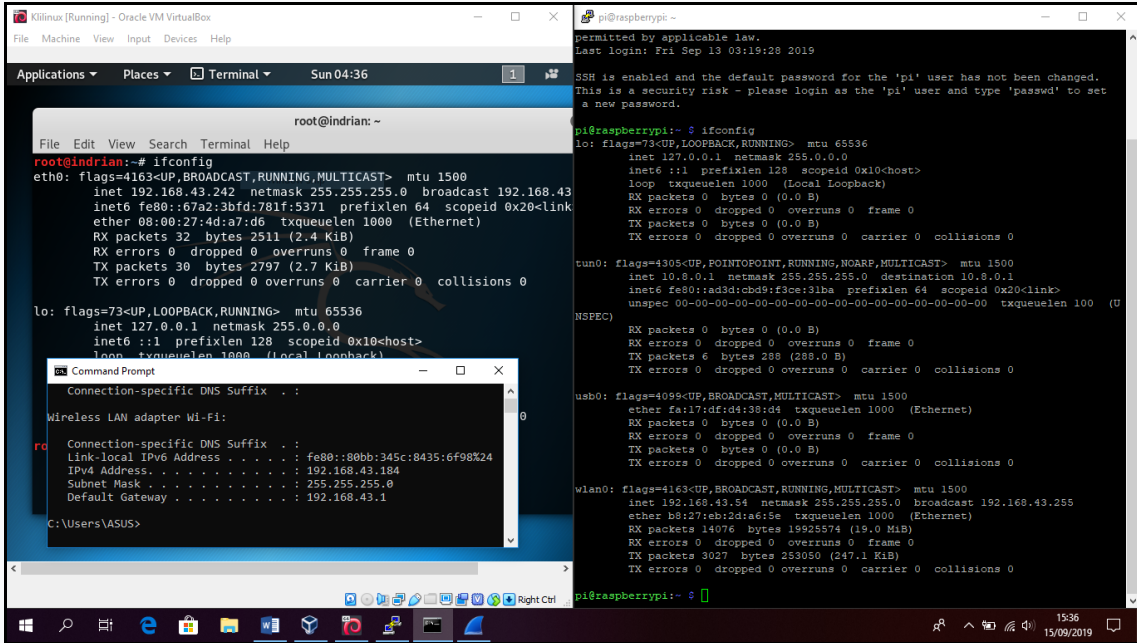
Ada beberapa penelitian yang menggunakan protokol *MQTT* untuk *internet of thing* seperti *monitoring UPS* dengan *MQTT Protocol*[6], *monitoring* kualitas udara dengan *MQTT Protocol*[7], dan *MQTT* untuk sistem automatisasi rumah[8], alasan penggunaan *MQTT protocol* pada penelitian ini karena sudah menjadi standar protokol IoT pada ISO/IEC 20922: 2016 (*Information technology - Message Queuing Telemetry Transport (MQTT) v3.1.1*) dan protokol ini digunakan secara luas untuk sistem IoT yang memiliki sumber daya terbatas karena beberapa alasan seperti ringan, bandwidth kecil, *opensource* dan mudah untuk diimplementasikan[9].

Kemudian untuk layanan keamanan data video streaming di sistem menggunakan *VPN* atau *virtual private network*. *VPN* adalah layanan komunikasi terenkripsi antar jaringan diseluruh dunia dengan menggunakan *tunneling internet protocol (IP)* dan seperti *internet*, dan koneksi *end-to-end* dibuat didalam tunnel[10][11]. Alasan menggunakan *Virtual Private Networks* pada penelitian ini karena *Virtual Private Networks (VPNs)* [12]saat ini menjadi metode yang paling mendunia yang digunakan untuk akses jarak jauh. Perusahaan cenderung melakukan ekspansi ke berbagai lokasi berbeda dan memiliki kantor cabang di banyak negara. *VPN* secara aman menyampaikan informasi (berbagi *file*, konferensi *video*, dan lain-lain di seluruh koneksi *Internet* ke pengguna jarak jauh, kantor cabang, dan mitra bisnis ke dalam jaringan perusahaan yang diperluas. *VPN* dibuat menggunakan koneksi khusus, protokol *tunneling virtual*, atau enkripsi trafik untuk membuat koneksi *point-to-point virtual*.

Modul utama yang digunakan pada sistem yang dibuat yaitu menggunakan mikroprosesor *Raspberry pi Zero W*. Alasan penggunaan *Raspberry pi Zero W* karena *Raspberry pi Zero W* berukuran kecil namun mempunyai fitur *wifi* dan *shield* kamera yang bisa digunakan untuk *streaming video* sehingga bisa dimanfaatkan intelijen untuk mengetahui aktifitas target yang diincar. Selain itu penggunaan *Raspberry* sudah banyak penggunaannya untuk berbagai aplikasi dan proyek seperti *video server* atau *real time video server*[13]. Penelitian lain juga membahas penggunaan *Raspberry* untuk mengontrol Robot[14],

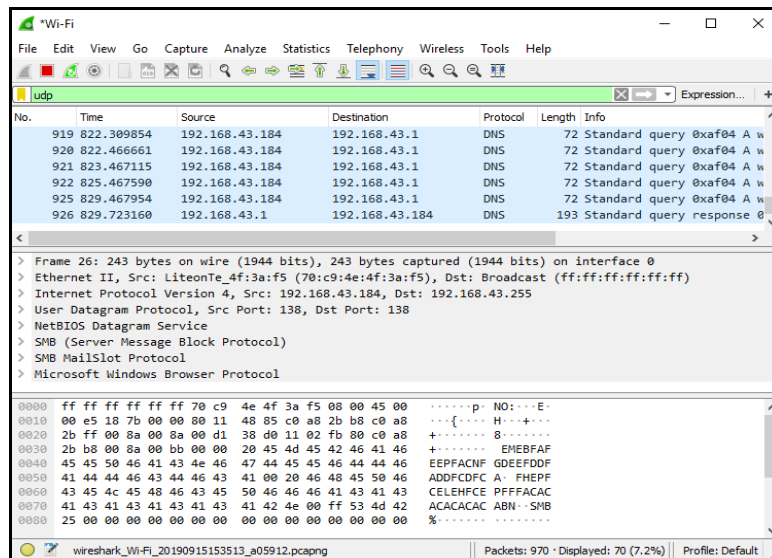
sehingga bisa dijadikan referensi untuk menggunakan *Raspberry pi* mengatur motor *servo* yang digunakan menggerakkan kamera sesuai arah yang diinginkan.

Ada beberapa teknik serangan pada pengiriman data antara lain dibahas pada yaitu *passive attack* dan *active attack*. *Passive attack* terdiri dari penyadapan dan analisis trafik jaringan, kemudian *Active attack* terdiri dari *masquerade attack*, *replay attack*, *modification*, dan *denial of service*[15]. Serangan yang bisa terjadi pada streaming video adalah penyadapan, analisis trafik, *masquerade attack*, *replay attack*, dan *modification*. Namun dengan implementasi *OpenVPN* serangan tersebut bisa ditanggulangi.



Gambar 15 Ip Address Windows, Raspberry, dan Kalilinux

Pada Gambar 15 merupakan gambar *Ip Address Windows, Raspberry, dan Kalilinux*. Skenario pengujian dan analisis yang dilakukan yaitu dengan menggunakan *Operating System* khusus untuk *penetration testing* yaitu *Kalilinux* yang dibuat satu jaringan dengan Klien *VPN Windows* dan *Server VPN Raspberry*. Pada *Kalilinux* terdapat *tools Wireshark* yang bisa digunakan untuk menyadap lalu lintas data *video streaming*. Namun dengan implementasi system ini *tools Wireshark* tidak bisa menyadap data *streaming video* yang dilakukan ketika *monitoring* target intelijen. Berikut *tools Wireshark*.



Gambar 16 Tools Wireshark dijalankan

Pada Gambar 16 merupakan gambar *tools Wireshark* ketika dijalankan. *Wireshark* akan memonitor trafik lalu lintas data di jaringan *wifi* yang terhubung dengan *Kalilinux*. Diharapkan dengan implementasi *OpenVPN* bisa mengamankan data *video streaming* target dari penyerang atau lawan.

V. KESIMPULAN

Implementasi *secure monitoring and detection for intelligence's target* dapat membantu dan memudahkan intelijen dalam melaksanakan operasi intelijen. Alat tersebut bekerja mendeteksi target intelijen dan mengirimkan informasi *video streaming* dari jarak jauh dengan keamanan data sensor dan data *video streaming* yang diamankan dengan teknik persandian. Teknik persandian yang digunakan yaitu dengan implementasi protokol *MQTT* dan *OpenVPN* pada lalu lintas data yang digunakan sehingga aman dari penyerang. Untuk kedepannya implementasi *secure monitoring and detection for intelligence's target* dapat dikembangkan untuk TNI AU khususnya di Dinas Pengamanan dan Persandian TNI AU.

DAFTAR PUSTAKA

- [1] W. I. N. Raspberry, P. I. Retro, and G. Kits, "You Must Make ! Pi Zero W," no. 61, 2017.
- [2] MakerBot Thingiverse, "Raspberry pi camera v2," p. 3280.
- [3] E. Systems, "ESP8266EX," 2019.
- [4] E. Micko, "PIR motion sensor," *US Pat. 7,579,595*, 2009.
- [5] Components101, "Servo Motor SG-90," *Components101.Com*, p. 180, 2017.
- [6] P. Alqinsi, I. J. Matheus Edward, N. Ismail, and W. Darmalaksana, "IoT-Based UPS Monitoring System Using MQTT Protocols," *Proceeding 2018 4th Int. Conf. Wirel. Telemat. ICWT 2018*, pp. 1–5, 2018.
- [7] S. Chanthakit and C. Rattanapoka, "Mqtt based air quality monitoring system using node MCU and node-red," *Proceeding 2018 7th ICT Int. Student Proj. Conf. ICT-ISPC 2018*, pp. 1–5, 2018.
- [8] R. K. Kodali and S. R. Soratkal, "MQTT based home automation system using ESP8266," *IEEE Reg. 10 Humanit. Technol. Conf. 2016, R10-HTC 2016 - Proc.*, 2017.
- [9] OASIS Open, "MQTT Version 3.1.1," *OASIS Stand.*, no. December, pp. 1–81, 2015.
- [10] J. Qu, T. Li, and F. Dang, "Performance evaluation and analysis of OpenVPN on Android," *Proc. - 4th Int. Conf. Comput. Inf. Sci. ICCIS 2012*, pp. 1088–1091, 2012.
- [11] J. Liu, Y. Li, N. Van Vorst, S. Mann, and K. Hellman, "A real-time network simulation infrastructure based on OpenVPN," *J. Syst. Softw.*, vol. 82, no. 3, pp. 473–485, 2009.
- [12] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment," *2015 Int. Conf. Comput. Commun. Secur. ICCCS 2015*, pp. 1–4, 2016.
- [13] F. Salih and S. A. Mysoon Omer, "Raspberry pi as a Video Server," *2018 Int. Conf. Comput. Control. Electr. Electron. Eng. ICCCEE 2018*, pp. 1–4, 2018.
- [14] Q. Dvhg, R. Xvlqj, R. Q. H. Dqg, R. Q. O. Frppxqlfdwlrq, and W. L. V. E. Wkh, "Android Based WI-FI Controlled Robot using Rasobery Pi," pp. 5–9, 2017.
- [15] W. Stallings, *Cryptography and Network Security (4th Edition)*. .

