Secure Personal Assistant Dengan Perintah Suara Berbasis Internet of Things (IoT) untuk Smart Office

Mohamad Ali Sadikin[1], Dedy Septono C. P[2]
Jurusan Teknik Persandian
Sekolah Tinggi Sandi Negara
Bogor, Indonesia
[1]mohamadalisadikin@gmail.com, [2]dedy.septono@stsn-nci.ac.id

***Abstrak*—Dalam paper ini, perangkat *secure personal assistant* dibangun pada Raspberry pi menggunakan perintah dan respon suara. Perangkat ini memiliki layanan umum seperti menunjukkan waktu saat ini, pengaturan alarm, *remainder*, membaca pembaruan berita, dan membaca email. Selain itu, perangkat ini memiliki fungsi khusus yaitu untuk sistem keamanan dan pemantauan, *secure* VOIP, *secure teleconference*, pemantauan suhu dan kelembaban, deteksi api otomatis. Perintah suara dan respon berbasis suara digunakan untuk memfasilitasi kontrol dan perintah perangkat *personal assistant*. Pemrosesan suara di perangkat ini menggunakan Google API. Untuk melakukan layanan, Raspberry Pi dilengkapi dengan mikrofon USB, modul kamera, sensor deteksi gerak, dan speaker. Selain itu perangkat juga dapat dikendalikan secara jarak jauh menggunakan perangkat Android. Protokol yang digunakan untuk melakukan transmisi data yaitu protokol *Message Queue Telemetry Transport* (MQTT). Kemudian, untuk mengamankan data yang dikirimkan *Virtual Private Network* (VPN). Hasil penelitian ini menunjukkan perangkat *personal assistant* dapat diimplementasikan dan dapat melakukan pekerjaan yang diperintahkan oleh pengguna. Selain itu, penerapan VPN SSL/TLS dapat mengamankan data yang dikirimkan seperti yang ditunjukkan pada paket yang ditangkap menggunakan Wireshark.**

Kata kunci— Personal Assistant, Smart Office, IoT, Security System, Monitoring System, Voice Recognition, voip, teleconference, VPN SSL/TLS;

I. PENDAHULUAN

Seiring perkembangan teknologi muncul perangkat *personal assistant*. *Personal assistant* merupakan perangkat yang berfungsi untuk mempermudah dan membantu pengguna dalam mencapai tujuannya. Penggunaan perangkat *personal assistant* akan memberikan *update* pengetahuan kepada pengguna [1]. Perkembangan perangkat *personal assistant* berbasis suara dapat dilihat seperti "Siri" pada *Apple*, "Cortana" pada *windows*, *Cubic*, *Echo*, *Jasper*, dan Jibo [25]. Perangkat tersebut masih bersifat umum karena memilik layanan yang bersifat umum. Dalam penelitian ini akan dikembangkan perangkat *personal assistant* yang dapat memberikan layanan keamanan.

Salah satu teknologi yang dapat digunakan untuk membangun *personal assistant* yaitu dengan menerapkan IoT [2]. IoT merupakan sebuah teknologi yang menghubungkan setiap *device* (perangkat) melalui internet untuk memudahkan kehidupan manusia, seperti *smart home*, *smart office*, *health care system*, *monitoring system* [3][4][5]. Perangkat yang digunakan dalam IoT memiliki *low-bandwith, low-repetition data capture*, dan *low-bandwidth data-usage appliances* untuk berkomunikasi dengan masing masing perangkat [6].

Dengan berkembangnya teknologi IoT, sehingga dapat mengintegrasikan perangkat-perangkat yang dikendalikan oleh *personal assistant*. Selain dapat memudahkan pekerjaan, namun terdapat tantangan besar seperti keamanan data, dan integrasi jaringan [7]. Keamanan dan privasi merupakan aspek yang sangat penting dalam IoT [8][9][10]. Terdapat beberapa kerawanan dalam komunikasi IoT yaitu *Eavesdropping attack, Impersonation attack, Man-in-the-middle attack, Denial of Service attack, Stolen smart device attack, Parallel session attack, Password change attack, Gateway node bypassing attack, Offline guessing attack* [5]. Oleh karena itu, diperlukan suatu solusi untuk mengatasi kerawanan tersebut. Pada IoT minimal harus menjamin layanan *Confidentiality, Integrity, Availability, Nonrepudiation, Authenticity*, dan *Privacy* [7][5][11].

Pada tahun 2014, *Organization for the Advancement of Structured Information Standards* (OASIS) mengeluarkan standar protokol untuk pertukaran data pada IoT yaitu *Message Queuing Telemetry Transport* [12][13]. MQTT merupakan *lightweight protocol* yang didesain secara khusus untuk pertukaran data pada IoT yang menjadi standar ISO/IEC 20922 tahun 2016 [14][15]. Akan tetapi protokol ini belum menjamin keamanan data pada IoT, maka dari itu disarankan untuk menambahkan pengamanan [16][17][18][19][20]. Salah satu pengamanan yang dapat diterapkan yaitu dengan menerapkan enkripsi atau *Transport Layer Security* [16][17][18][19][20].

Berdasarkan permasalahan diatas, pada penelitian ini akan dibangun prototipe *personal assistant* berbasis IoT menggunakan Raspberry Pi 3 Model B, Node MCU, dan *smartphone* android. Raspberry Pi 3 Model B dipilih karena memiliki kelebihan sebagai perangkat *personal assistant* yaitu memiliki kemampuan komputasi yang cukup, lebih hemat

penggunaan komponen, lebih ringan, dan lebih hemat energi sehingga cocok digunakan sebagai perangkat *secure personal assistant* berbasis IoT [3][21]. Node MCU dipilih sebagai perangkat IoT yang didesain secara kusus untuk menangani sensor pada IoT.

Prototipe yang akan dibangun memiliki kemampuan untuk selalu aktif mendengarkan instruksi dan memecahkan masalah spesifik yang diberikan oleh pengguna. Perangkat ini memiliki kemampuan seperti perangkat asisten pribadi secara umum yang menunjukkan waktu saat ini, pengaturan alarm, pengaturan sisa, membaca pembaruan berita, menyediakan data, dan membaca email, ramalan cuaca, dan *chat bot*. Selain kemampuan di atas, karena perangkat yang dibangun adalah perangkat yang dirancang khusus untuk *secure personal assistant* pada *smart office* maka perangkat tersebut memiliki kemampuan utama yang dapat menyediakan sistem pemantauan yang aman, sistem keamanan, *secure* VOIP, pemantauan suhu dan kelembaban, deteksi api otomatis, pusat komando untuk lampu dan mengunci pintu, *secure teleconference*. Untuk keamanan layanan ini menggunakan teknologi *Virtual Private Network* dengan *library* Open SSL.

Selanjutnya, untuk memudahkan mengendalikan perangkat utama, kontrol menggunakan smartphone akan dikembangkan. Smartphone akan digunakan untuk menghubungkan antara pengguna dan perangkat. Pengguna dapat memberi perintah dengan suara atau teks. Selain itu, smartphone akan digunakan untuk mengontrol layanan lain, seperti pemantauan yang aman, suhu dan kelembaban, *chat bot*, deteksi api otomatis, dan pusat perintah.

Virtual Private Network (VPN) memperluas jaringan *private* di seluruh jaringan publik, seperti Internet. Layanan keamanan yang dapat disediakan oleh VPN adalah kerahasiaan, keaslian, dan integritas data sehingga data yang dikirimkan melalui VPN dapat menghindari risiko intersepsi oleh pihak yang tidak berwenang. Terdapat tiga protokol VPN yang sering digunakan, yaitu *point to point tunneling protocol* (PPTP) VPN, IPSec VPN, dan SSL VPN. OpenVPN memiliki keuntungan yang dapat dikonfigurasi sesuai dengan kebutuhan pengguna. Di dalam OpenVPN, ada pustaka OpenSSL yang berisi semua layanan kriptografi, seperti daftar algoritme yang digunakan untuk enkripsi, tanda tangan digital, dan sertifikat digital [22].

II. LANDASAN TEORI

A. *Smart Office*

Sistem *smart office* adalah sistem aplikasi gabungan antara teknologi dan pelayanan yang di khususkan pada suatu kenyamanan kantor dengan fungsi yang bertujuan untuk meningkatkan efisiensi, keamanan pemilik serta kariawannya.

Dalam penerapan *smart office* adalah menyatukan seluruh komponen koneksi komunikasi–baik itu data dan suara dengan manajemen gedung yang sebelumnya terpisah sehingga lebih mahal dan menciptakan pulau-pulau sistem. Integrasi berbagai komponen tersebut memanfaatkan teknologi IP sebagai infrastruktur yang diatasnya dikembangkan dengan BAS dan berbagai peranti akses dan aplikasi seperti "*Facility Management*," "*Maintenance Management*," dan "*IT Network Management*."

B. *Personal Assistant*

Personal assistant adalah sebuah perangkat sistem yang digunakan untuk membantu pengguna dalam mencapai tujuanya dengan efisien. Sebuah *personal assistant* secara umum memiliki fungsi untuk membantu pengguna dalam menyelesaikan pekerjaan.

Beberapa perangkat *personal assistant* yang mirip dengan penelitian kami yaitu "Jasper" [12]. *Personal assistant open source* yang dikendalikan dengan suara perintah yang dieksekusi pada Raspberry Pi. Mereka memiliki fungsi yang berbeda seperti cek email, atau cuaca atau bahkan notifikasi "Facebook". Sedangkan untuk *personal assistant non-open source* sperti "Cubic" [13] atau "Echo" [14] dari "Amazon".

Selain itu, sebuah *personal assistant* yang canggih yang terlihat seperti penelitian kami yaitu "Jibo" [15] yang sedang dalam pengembangan. Yang ini seperti robot sosial cerdas yang memungkinkan menerima acara kalender, menanyakan sesuatu yang dapat ditanyakan seperti di “Siri” atau menyimpan beberapa percakapan atau menyarankan hal-hal tertentu tergantung dari preferensi Anda. Perbedaan utama dalam hal "Jasper" adalah memiliki kamera yang mampu melacak pengguna dan jika pengguna meminta foto, maka perangkat akan menyediakan foto tersebut.

Semua di atas adalah pengembangan perangkat *personal assistant*. Berdasarkan penelitian sebelumnya tidak ada perangkat asisten pribadi yang secara khusus menerapkan fitur keamanan. Oleh karena itu, dalam penelitian ini akan diimplementasikan asisten pribadi pada Raspberry pi dengan input berupa perintah suara dan output dari respon suara. Perangkat asisten pribadi ini selain memiliki layanan umum juga memiliki layanan khusus yaitu sebagai perangkat keamanan di kantor pintar dan sistem pemantauan untuk mengetahui kondisi dikantor. Selain itu, perangkat ini juga akan menerapkan teknologi VPN untuk mengamankan proses transmisi informasi dari perangkat asisten pribadi ke pengguna akhir dan sebaliknya. VPN yang digunakan adalah open source yaitu OpenVPN.

C. *Internet of Things* (IoT)

IoT merupakan sebuah teknologi yang menghubungkan setiap *device* (perangkat) melalui internet untuk memudahkan kehidupan manusia, seperti *smart home*, *health care system*, *monitoring system* [3][4][5]. IoT bekerja menggunakan sensor untuk mengumpulkan informasi [23]. Perangkat yang digunakan dalam IoT memiliki *low-bandwith, low-repetition data capture*, dan *low-bandwidth data-usage appliances* untuk berkomunikasi dengan masing masing perangkat [6].

IoT dapat dibagi menjadi 6 elemen yang dapat digunakan untuk mempermudah konsep dari IoT, yaitu *identification, sensing, communication, computation, services and semantics*. Selain elemen pembangun dalam IoT terdapat hal yang perlu diperhatikan pada IoT yaitu terkait isu keamanan. Keamanan dan privasi pada IoT merupakan hal yang mendasar untuk melindungi data yang bersifat rahasia. Seperti kebutuhan akan kerahasiaan data dan autentikasi, kontrol akses terhadap

jaringan IoT, privasi dan kepercayaan antara *user* dan perangkat, serta menjalankan kebijakan terkait privasi dan keamanan [24].

D. Protokol *Message Queue Telemetry Transport* (MQTT)

MQTT merupakan sebuah protokol komunikasi data *machine to machine* (M2M) yang bersifat *lightweight* atau ringan [12]. MQTT memiliki *header* pesan berukuran kecil yaitu hanya sebesar 2 *bytes* untuk setiap jenis data, sehingga dapat bekerja pada lingkungan yang memiliki *power* dan *bandwidth* yang rendah [12]. MQTT bersifat ringan, terbuka, sederhana, dan didesain agar mudah diimplementasikan. Karakteristik ini membuat MQTT dapat digunakan di banyak situasi, termasuk penggunaanya dalam komunikasi *Internet of Things* (IoT). Selain itu protokol ini juga menjamin terkiriminya semua pesan walaupun koneksi terputus sementara. Protokol MQTT merupakan protokol berbasis *client server* dengan metode *publish*/*subscribe* untuk metode komunikasinya.

E. Virtual Private Network

Virtual Private Network atau VPN adalah suatu jaringan privat yang menggunakan infrastruktur telekomunikasi publik seperti jaringan internet untuk saling bertukar informasi. VPN banyak digunakan oleh suatu organisasi atau perusahaan yang membutuhkan akses eksternal menuju ke jaringan internalnya secara aman. Layanan keamanan informasi yang paling mendasar untuk diimplementasikan pada VPN adalah enkripsi, otentikasi, dan integritas data. Sehingga seluruh data yang ditransmisikan melalui VPN biasanya terenkripsi untuk mengantisipasi adanya lawan dengan akses ke internet dapat melakukan *eavesdropping* terhadap data yang dipertukarkan melalui jaringan publik. Tanpa adanya otentikasi, pihak-pihak atau entitas yang tidak sah juga dapat bertindak seperti pegawai perusahaan kemudian masuk ke jaringan internal. Integritas data diperlukan karena paket yang dipertukarkan melalui jaringan publik berpotensi besar mengalami perubahan atau modifikasi oleh pihak yang tidak memiliki otoritas.

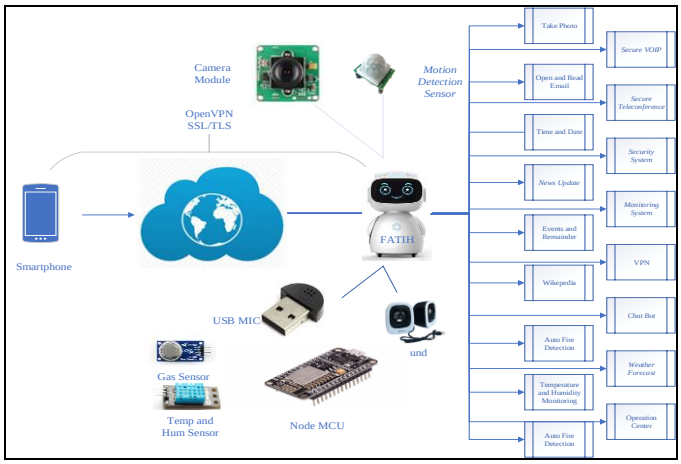
OpenVPN merupakan salah satu perangkat lunak VPN yang berbasis protokol SSL atau biasa disebut dengan SSL VPN. Protokol ini cukup banyak digunakan untuk mengamankan transaksi data melalui internet. Kuat dan cukup mudah untuk dipelajari oleh pengguna baru, selain itu juga lebih sederhana untuk diimplementasikan dan dimanajemen oleh seorang *administrator*.

III. IMPLEMENTASI *SECURE PERSONAL ASSISTANT* BERBASIS IOT

A. Deskripsi Umum Sistem

Sistem ini didasarkan pada arsitektur perangkat lunak modular. Setiap modul independen dari yang lain dan memiliki fungsi yang sesuai dalam hubungannya dengan proyek. Ini memungkinkan seseorang untuk memilih opsi yang berbeda seperti menambahkan atau menghapus modul tertentu yang dapat menyebabkan kesalahan pada keseluruhan sistem. Jika beberapa modul tidak berfungsi dengan benar, itu bisa diubah untuk yang lain atau dapat secara otomatis diubah ke opsi lain di dalam modul.

Dalam kasus ini modul perangkat *personal assistant* seperti yang dapat dilihat pada Gambar 1, jika beberapa sub-modul tidak berfungsi seperti yang diharapkan, sistem akan mengelola kesalahan ini dan memicu untuk memberikan notifikasi pengguna bahwa sub-modul yang dipilih tidak berfungsi dengan baik.



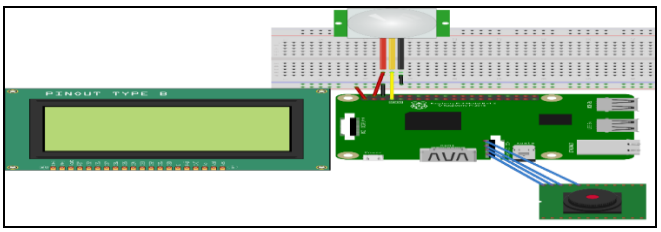
Gambar 1. Gambaran umum sistem *personal assistant* berbasis IoT untuk *smart office*

Pada Gambar 1. menunjukkan gambaran umum dari sistem yang dibangun. Sistem yang dibangun terdiri dari perangkat utama yaitu perangkat *personal assistant* (PA) yang dibangun menggunakan Raspberry Pi. Perangkat utama akan memiliki berbagai layanan umum seperti pembaruan berita, membuka dan membaca email, waktu dan tanggal, acara dan jadwal kegiatan, wikipedia, mengambil foto, mengakses layanan menggunakan *smartphone*, prakiraan cuaca [25] dan layanan yang dirancang khusus untuk penggunaan kantor pintar seperti *secure* VOIP, telekonferensi yang aman, sistem keamanan dan pemantauan, dan VPN [22], pemantauan suhu dan kelembaban, deteksi api otomatis, pusat kendali untuk lampu dan mengunci pintu.

Selanjutnya, perangkat utama akan dikendalikan oleh dua metode. Metode pertama adalah ketika pengguna berada dalam satu kondisi ruangan yang mencapai untuk memberikan perintah suara. Dalam kondisi ini pengguna mengontrol perangkat utama dengan memberikan perintah suara dan mendapatkan respons juga dalam bentuk suara dari perangkat utama. Metode kedua adalah ketika pengguna tidak dalam satu ruangan. Dalam kondisi ini, pengguna dapat memberikan perintah suara ke perangkat utama menggunakan bantuan telepon pintar yang terintegrasi.

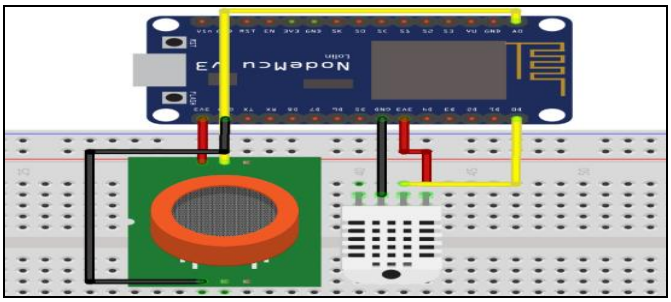
B. Desain Perangkat Keras

Dalam penelitian ini arsitektur perangkat keras dirancang menggunakan *board* utama yaitu Raspberry Pi 3 Model B. Perancangan perangkat keras ini dirancang menggunakan Fritzing. Raspberry Pi digunakan sebagai perangkat *personal assistant* utama. Raspberry Pi terhubung ke perangkat lain seperti mikrofon, speaker, kamera, dan sensor deteksi gerakan. Gambar 2 menunjukkan desain arsitektur perangkat keras.



Gambar 2. Desain perangkat keras utama

Berdasarkan Gambar 2, dalam desain utama perangkat ini menggunakan Raspberry Pi 3 Model B. Raspberry Pi terhubung dengan sensor PIR melalui pin GPIO 4, pin 5 V, dan pin GND. Perangkat yang terhubung ke Raspberry Pi melalui Port USB adalah USB MIC, Power Speaker, webcam, dan Power LCD. Layar sentuh LCD terhubung ke Raspberry via HDMI. Sementara kamera terhubung dengan Raspberry melalui port kamera.



Gambar 3. Desain perangkat keras pada Node MCU

Dalam penelitian ini *node* akan dibangun menggunakan Node MCU ESP8266 versi 3.0. Node MCU ESP8266 memiliki sejumlah 10 pin digital, 1 pin analog, 1 RX dan 1 pin TX. Node MCU akan terhubung dengan relay yang mengakomodasi lima perangkat. Dalam penelitian ini pin digital yang digunakan adalah 10 dari 15 pin pada Node MCU ESP8266. Berikut ini daftar Pin pada Node MCU yang digunakan sebagai input dan output untuk sensor dan perangkat IoT.

C. Desain Perangkat Lunak

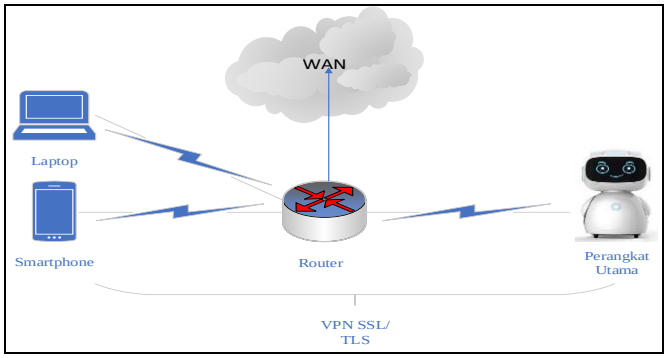
Selain OpenVPN SSL ada perangkat lunak yang dibangun di perangkat berbasis Android. Perangkat ini dirancang menggunakan pemrograman XML di Android Studio IDE. Inilah desain perangkat lunak pada *smartphone*.

Gambar 4. Desain perangkat lunak

Berdasarkan Gambar 4, perangkat lunak ini dirancang untuk memiliki tampilan depan dan tampilan menu utama. Perangkat lunak yang dirancang di android digunakan sebagai pengendali jarak jauh perangkat utama. Perangkat ini digunakan untuk menyederhanakan pengguna dan mendukung mobilitas pengguna perangkat.

D. Desain Jaringan

Keamanan jaringan dalam penelitian ini dirancang menggunakan teknologi VPN. Teknologi VPN digunakan karena memberikan layanan seperti kerahasiaan, otentikasi, integritas data, dan tahan terhadap serangan replay. VPN digunakan untuk membuat terowongan antara perangkat pengguna akhir dan perangkat asisten pribadi. Terowongan akan digunakan untuk mengirimkan data dan informasi kepada pengguna. Gambar 5 menunjukkan desain keamanan jaringan dalam sistem ini.



Gambar 5. Desain jaringan

Gambar 5. menunjukkan bahwa dalam penelitian ini akan diimplementasikan SSL/TLS VPN. SSL / TLS VPN digunakan untuk mengamankan transmisi data antar perangkat. Layanan ini dibangun dengan menerapkan OpenVPN SSL. Server VPN akan dibangun di perangkat Raspberry Pi dan Laptop.

E. Implementasi

Semua implementasi dan fungsionalitas dirancang menggunakan pemrograman python untuk bekerja dalam kompatibilitas Raspberry Pi [21], pemrograman C di Node MCU dan Java di android. Namun, banyak konfigurasi dan paket yang dipasang di Raspberry Pi untuk mengatur lingkungan yang benar di mana asisten akan dieksekusi.

Untuk prototipe Raspberry Pi, beberapa periferal ditambahkan:

- USB Microphone
- Speakers
- Camera
- Motion detection sensor

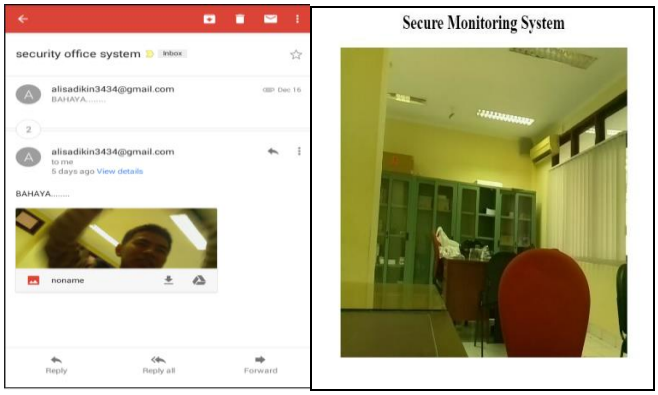
Terlebih lagi, ada beberapa perangkat lunak yang harus diinstal:

- Speech Recognition
- Web browser library
- Wikipedia
- Google APIs Text to Speech
- Telegram API
- Open VPN SSL/TLS

Untuk Node MCU, beberapa sensor ditambahkan:

- DHT11 (Temp and Humid Sensor)
- MQ-2 Sensor (Fire Detection)

Gambar 4 dan 5 menunjukkan hasil implementasi dari perangkat *personal assistant* untuk keamanan dan sistem pemantauan. Sistem keamanan akan mengirimkan pemberitahuan kepada pengguna email ketika ada orang yang masuk kedalam ruangan.



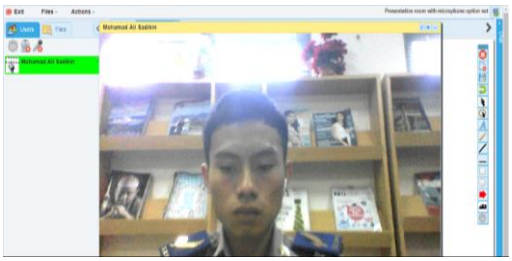
Gambar 6. Sistem keamanan dan *secure monitoring*

Sistem pemantauan mengirimkan video *real-time* dari perangkat *personal assistant* ke perangkat pengguna seperti laptop atau ponsel cerdas. Video ditransmisikan dengan teknologi VPN. VPN akan membuat terowongan dari perangkat asisten pribadi ke perangkat pengguna. Jadi, data yang dikirimkan aman terhadap penyerang. Penyerang tidak akan mendapatkan apa-apa ketika melakukan *sniffing* paket data dalam lalu lintas. Port *default* yang digunakan adalah 5000. Berikut adalah IP VPN *server* yang telah digunakan pada Raspberry Pi.

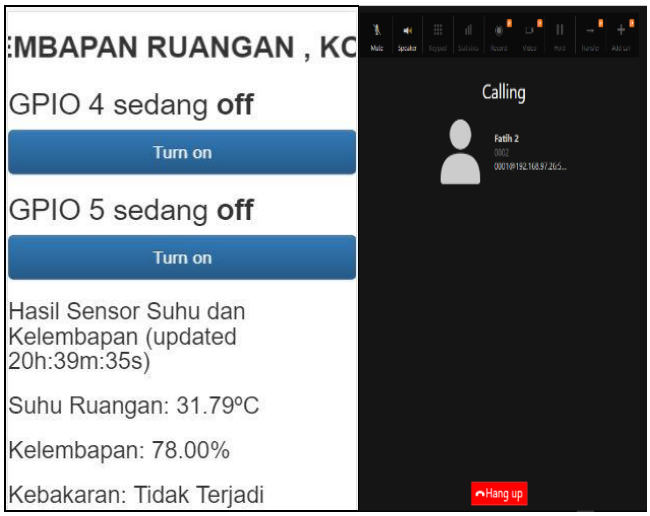
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.8.0.1  P-t-P:10.8.0.1  Mask:255.255.255.0
          inet6 addr: fe80::b6e2:a970:430a:9e0f/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:192 (192.0 B)
```

Gambar 7. *Secure* Teleconference

Berdasarkan Gambar 7 bahwa Raspberry Pi memiliki IP yaitu 10.8.0.1 yang merupakan IP VPN *server*. Setiap perangkat akan menggunakan IP tersebut untuk mengakses setiap layanan yang disediakan.



Gambar 8. *Secure* Teleconference



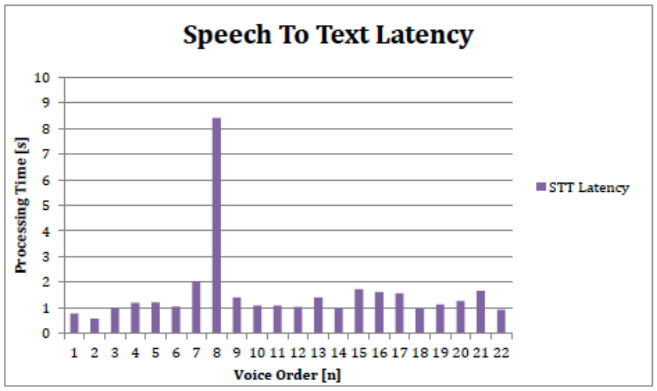
Gambar 9. Sistem kendali suhu dan kelembapan, deteksi kebakaran dan *secure* VOIP

IV. HASIL DAN ANALISIS

Pada bagian ini, kita membahas hasil analisis asisten pribadi implementasi berdasarkan IoT di Smart Office Berdasarkan Raspberry Pi, Voice Command, dan Smartphone untuk mengontrol *Over* MQTT [12][13][14] dan VPN. Analisis dilakukan dengan menggunakan analisis sistem dan pengujian keamanan. Pertama, kami melakukan analisis sistem PA.

A. Deskripsi Umum Sistem

Beberapa keterbatasan dalam kapasitas sistem kami untuk berinteraksi dengan pengguna dengan respon cepat diharapkan. Asisten pribadi sangat bergantung pada API dan layanan eksternal seperti Google atau Wolfram. Hambatan utama dari kecepatan interaksi ini diberikan oleh subsistem Google STT yang bertanggung jawab atas pengenalan urutan suara.



Gambar 10. Waktu STT

Seperti yang bisa dilihat pada Gambar 9, dibutuhkan rata-rata, satu detik. Meskipun dalam beberapa kesempatan atau tergantung pada koneksi internet atau layanan Google, itu bisa memakan waktu hingga 8 detik. Beberapa pertimbangan untuk dipertimbangkan adalah waktunya sangat bergantung pada berat audio yang dikirim ke *server* Google. Artinya jika perintah suara terlalu panjang, asisten pribadi akan membutuhkan waktu lebih lama untuk memproses pesanan ini.

B. *System Testing*

Pengujian sistem dilakukan dengan memeriksa pemenuhan semua persyaratan fungsional dan non-fungsional dari aplikasi. Pengujian dilakukan dengan membandingkan hasil implementasi dengan kebutuhan fungsional dan non fungsional. Percobaan pengujian dialkukan dengan mencoba setiap layanan yang terdapat pada perangkat. Tabel 1 menunjukkan hasil pengujian persyaratan fungsional, sedangkan hasil tes terhadap persyaratan non-fungsional ditunjukkan oleh Tabel 2

TABEL I. HASIL *SYSTEM TESTING* PADA KEBUTUHAN FUNGSIONAL

No	Kebutuhan Fungsional	Hasil
1	Perintah berbasis suara	✓
2	Respon suara	✓
3	Registrasi	✓
4	Login	✓
5	Sistem Keamanan	✓
6	*Secure monitoring*	✓
7	*Weather forecast*	✓
8	*Reminder*	✓
9	Pusat kendali	✓
10	*Secure* VOIP	✓
11	*secure teleconference*	✓
12	VPN	✓
13	Kendali melalui *smartphone*	✓
14	Pemantauan suhu dan kelembapan ruangan	✓
15	Otomasi deteksi kebakaran	✓
16	*Update* berita	✓

TABEL II. HASIL *SYSTEM TESTING* PADA KEBUTUHAN NON FUNGSIONAL

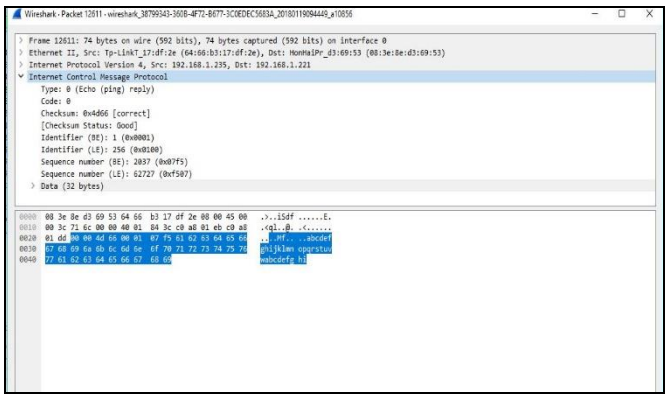
No	Kebutuhan Non-Fungsional	Hasil
1	Animasi	✓
2	Program C, python, dan web.	✓
3	*OpenVPN* pada *Raspberry Pi*	✓
4	*Secure* VOIP menggunakan RasPBX dan Arterisk	✓
5	*Secure* VOIP client menggunakan *open source ZOIP*	✓
6	*Secure teleconference* dibangun menggunakan *open meeting apache*	✓
7	*Secure VOIP*, *secure teleconference* menggunakan laptop.	✓

Pengujian Sistem terdiri dari dua tes, yaitu pengujian kebutuhan fungsional dan non-fungsional. Dari pengujian yang dilakukan, semua persyaratan sistem dapat dipenuhi, sehingga sistem telah sesuai dengan kebutuhan dalam proses implementasi.

C. *Security Testing*

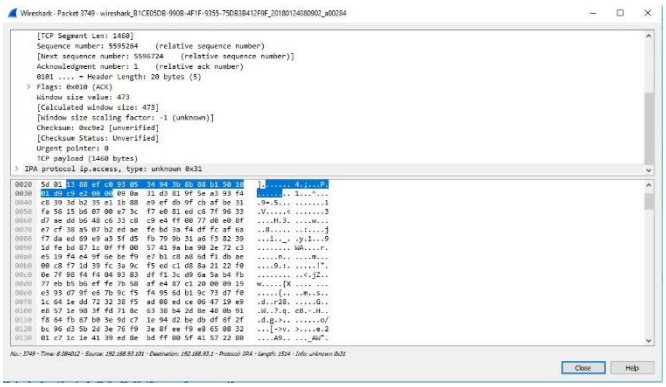
Pengujian keamanan dalam penelitian ini digunakan untuk membuktikan penerapan teknologi VPN untuk mengamankan video yang dikirim dari perangkat asisten pribadi ke perangkat pengguna. Pengujian keamanan dilakukan dengan melakukan *sniffing* lalu lintas paket data menggunakan Wireshark. Wireshark digunakan untuk menangkap paket yang dikirimkan.

Gambar 10 menunjukkan paket yang ditangkap sebelum VPN SSL/TLS diimplementasikan. Paket ditampilkan dalam bentuk *plaintext*. Sehingga penyerang dapat membaca informasi yang dikirimkan.



Gambar 11. Paket data yang ditangkap sebelum implementasi VPN

Kemudian Gambar 11 menunjukkan paket data yang ditangkap setelah VPN SSL/TLS diimplementasikan. Paket ditampilkan dalam bentuk *ciphertext*. Sehingga penyerang tidak dapat membaca informasi yang ditransmisikan.



Gambar 12. Paket data yang ditangkap sebelum implementasi VPN

V. KESIMPULAN

Perangkat *personal assistant* berhasil diimplementasikan pada Raspberry Pi. Perangkat ini perintah dengan suara dan respon juga dengan suara. Perangkat dapat bekerja sesuai masukan pengguna. Berdasarkan pengujian, bahwa perintah suara dapat dikenali dengan menggunakan *library* Google API. Selanjutnya, VPN SSL/TLS berhasil diterapkan untuk mengamankan informasi dan data yang ditransmisikan dari perangkat *personal assistant* ke perangkat pengguna. Berdasarkan hasil *system testing* menunjukan bahwa sistem telah memenuhi kebutuhan fungsional dan non fungsional. Sedangkan hasil *security testing* menunjukan bahwa paket data yang terkirim sudah terenkripsi, hal tersebut dapat dilihat dari paket yang tertangkap melalui *sniffing* Wireshark.

Pada penelitian kedepan dapat dikombinasikan dan dikembangkan dengan komunikasi terpadu dan *artificial intelligent* (AI).

UCAPAN TERIMA KASIH

Terimakasih penulis ucapkan kepada Sekolah Tinggi Sandi Negara yang telah mendukung penelitian ini.

REFERENSI

[1] A. Hussain, "Personal Smart Assistant for Digital Media and Advertisement," no. March, 2013.

[2] J. Santos, et al., "Intelligent Personal Assistants Based on Internet of Things Approaches," *IEEE Syst. J.*, pp. 1–10, 2016.

[3] A. Glória, F. Cercas, and N. Souto, "Design and implementation an IoT gateway to create smart environments," *Procedia Comput. Sci.*, vol. 109, pp. 568–575, 2017.

[4] A. Al-fuqaha et al., "Internet of Things : A Survey on Enabling Technologies , Protocols and Applications," *IEEE Commun. Surv. Tutor.*, 2015.

[5] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 0, pp. 1–16, 2017.

[6] W. Stalling, *Security for the Internet of Things*. Elsevier Inc., 2017.

[7] L. Da Li, Shancang and Xu, *Securing the Internet of Things*. Cambridge, MA 02139, United States: Elsevier Inc. All rights reserved, 2017.

[8] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, no. February, pp. 17–31, 2015.

[9] C. Moratelli et al., "Invited Talk Paper Embedded Virtualization for the Design of Secure IoT Applications," in *Proceedings of the 27th International Symposium on Rapid System Prototyping: Shortening the Path from Specification to Prototype*, 2016, pp. 2–6.

[10] N. T. and I. A. U. S. D. of Commerce, *The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World"* , no. June. USA, 2016.

[11] A. R. Sfar et al., "A Roadmap for Security Challenges in Internet of Things," *Digit. Commun. Networks*, 2017.

[12] [OASIS, "MQTT Version 3.1.1," 2014.

[13] Mqtt.org, "Documentation _ MQTT," 2017. [Online]. Available: http://mqtt.org/documentation. [Accessed: 22-Aug-2017].

[14] ISO, "ISO_IEC 20922 2016 - Information technology -- Message Queuing Telemetry Transport (MQTT) v3.1.1," *ISO/IEC 20922:2016*, 2016. [Online]. Available: https://www.iso.org/standard/69466.html. [Accessed: 22-Aug-2017].

[15] M. L. Corbin, "MQTT is the de-facto standard and ISO standard for messaging protocols," *The developerWorks Blog*, 2016. [Online]. Available: https://developer.ibm.com/dwblog/2016/mqtt-de-facto-standard-iso-messaging/.

[16] IETF, "A TLS/DTLS 1.2 Profile for the Internet of Things draft-ietf-dice-profile-07," 2015.

[17] Symantec, "An Internet of Things Reference Architecture," 2017.

[18] A. Gantait, J. Patra, and A. Mukherjee, "Design and build secure IoT solutions , Part 1 : Securing IoT devices and gateways," 2017.

[19] T. H. Team, "MQTT Security Fundamentals TLS/SSL," *MQTT Security Fundamentals*, 2017. [Online]. Available: http://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl. [Accessed: 22-Aug-2017].

[20] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things," 2015.

[21] C. Bell, *Beginning Sensor Networks with Arduino and Raspberry Pi*. Apress, 2013.

[22] W. Stallings, *Cryptography and Network Security : Principle and Practice*, Seventh. 2017.

[23] C. Bude and A. K. Begstrand, "Internet of Things Internet of Things Exploring and Securing a Future Concept Industrial adviser," KTH ROYAL INSTITUTE OF TECHNOLOGY, 2015.

[24] S. Sicari et al., "Security , privacy and trust in Internet of Things : The road ahead," *Comput. Networks J.*, vol. 76, pp. 146–164, 2015.

[25] González, M. C. T. (2016). *My Personal Assistant*. Universitat Politècnica de Catalunya.