

Saran Pengembangan Infrastruktur Jaringan

“Sistem perekam Detak Jantung Berbasis *Internet Of Things (IoT)* dengan Menggunakan *Pulse Heart Rate Sensor*”

Gambaran:

Tujuan:

- Menguji sistem perekam detak jantung berbasis IoT dan membandingkannya dengan oximeter.

Metode:

- Merancang dan membangun sistem perekam detak jantung menggunakan sensor Pulse Heart Rate, ESP8266, modul Sd-Card, dan aplikasi Blynk.
- Menguji sistem dengan 5 orang sampel untuk mengukur detak jantung dalam kondisi santai, makan, dan setelah olahraga.
- Membandingkan hasil pengukuran sistem dengan hasil pengukuran oximeter.

Hasil:

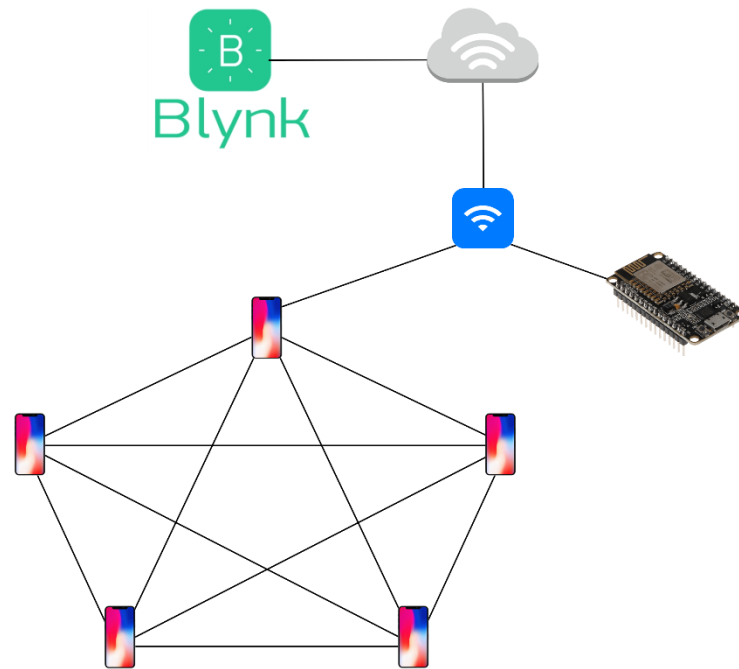
- Sistem perekam detak jantung dapat mengukur detak jantung dengan akurasi yang cukup baik, dengan rata-rata selisih 1-2 bpm dibandingkan dengan oximeter.
- Detak jantung meningkat pada saat setelah olahraga yaitu 114,4 bpm dibandingkan dengan saat makan 90,8 bpm dan saat santai 66,6 bpm.
- 60% (3 dari 5 orang) yang memiliki detak jantung yang sama baik menggunakan alat maupun menggunakan oxymeter.

Saran Pengembangan:

- Gunakan jaringan mesh untuk meningkatkan jangkauan dan keandalan sistem.
- Gunakan teknologi IoT berdaya rendah untuk mengurangi konsumsi daya dan memperpanjang masa pakai baterai.
- Gunakan platform cloud yang aman untuk menyimpan dan menganalisis data detak jantung pengguna.

Topologi Jaringan:

- Topologi mesh direkomendasikan untuk sistem ini karena ideal untuk aplikasi IoT di mana diperlukan jangkauan yang luas dan keandalan yang tinggi.



Gambar 1. Topologi Jaringan Mesh

1. Penggunaan Jaringan Mesh:

- Alasan: Jaringan mesh memungkinkan setiap perangkat dalam jaringan untuk menjadi node yang terhubung langsung satu sama lain, bukan hanya ke satu titik akses pusat. Hal ini meningkatkan jangkauan dan keandalan jaringan, karena data dapat mengalir melalui rute terbaik yang tersedia di antara node-node tersebut. Jika salah satu node gagal atau terputus, jaringan masih tetap berfungsi karena node lain dapat menangani aliran data.
- Dampak: Dengan menggunakan jaringan mesh, sistem akan lebih dapat diandalkan, mengurangi risiko kegagalan atau kehilangan konektivitas, dan memberikan cakupan yang lebih luas tanpa harus mengandalkan poin akses tunggal.

2. Penggunaan Teknologi IoT Berdaya Rendah:

- Alasan: Teknologi Internet of Things (IoT) berdaya rendah (low-power) memungkinkan perangkat untuk beroperasi dengan konsumsi daya yang minimal, yang sangat penting untuk meningkatkan masa pakai baterai perangkat. Ini sangat berguna dalam aplikasi yang membutuhkan perangkat yang dapat beroperasi untuk jangka waktu yang lama tanpa harus sering mengganti atau mengisi ulang baterai.
- Dampak: Dengan menggunakan teknologi IoT berdaya rendah, masa pakai baterai perangkat dapat diperpanjang, mengurangi gangguan karena

penggantian baterai yang sering, serta meningkatkan kenyamanan dan kepraktisan penggunaan perangkat.

3. Penggunaan Platform Cloud yang Aman:

- Alasan: Platform cloud menyediakan infrastruktur yang fleksibel dan dapat diakses dari mana saja, memungkinkan penyimpanan dan analisis data secara efisien. Memilih platform cloud yang aman sangat penting untuk melindungi data sensitif, seperti data detak jantung pengguna, dari serangan dan kebocoran data.
- Dampak: Dengan menggunakan platform cloud yang aman, data detak jantung pengguna akan terlindungi dengan baik, mencegah akses yang tidak sah atau kebocoran data. Selain itu, analisis data detak jantung dapat dilakukan dengan lebih efektif dan responsif dengan infrastruktur yang skalabel dan kuat yang disediakan oleh platform cloud.

Gambaran dan Saran Pengembangan Infrastruktur Jaringan

“Utilizing neural networks with CICIDS2018 dataset for detecting brute force attack anomalies in intrusion detection systems”

Gambaran:

Jurnal "Pemanfaatan Jaringan Syaraf dengan Dataset CICIDS2018 untuk Mendeteksi Anomali Serangan Brute Force pada Intrusion Detection System" memberikan kontribusi yang berharga dalam bidang deteksi intrusi jaringan. Penggunaan jaringan syaraf untuk mengidentifikasi pola serangan brute force menunjukkan potensi yang menjanjikan dalam meningkatkan akurasi dan efisiensi Intrusion Detection System (IDS).

Penelitian ini memiliki beberapa kelebihan, di antaranya:

- **Pendekatan berbasis jaringan syaraf:** Penggunaan jaringan syaraf memungkinkan model untuk belajar dari data dan mengidentifikasi pola serangan brute force dengan lebih baik dibandingkan metode tradisional seperti deteksi berbasis signature.
- **Penggunaan dataset CICIDS2018:** Dataset CICIDS2018 merupakan dataset benchmark yang banyak digunakan dalam penelitian deteksi intrusi, sehingga hasil penelitian ini dapat dibandingkan dengan penelitian lain.
- **Evaluasi yang komprehensif:** Penelitian ini mengevaluasi model jaringan syaraf dengan berbagai metrik, seperti akurasi, presisi, recall, dan F1 score, sehingga memberikan gambaran yang komprehensif tentang kinerja model.

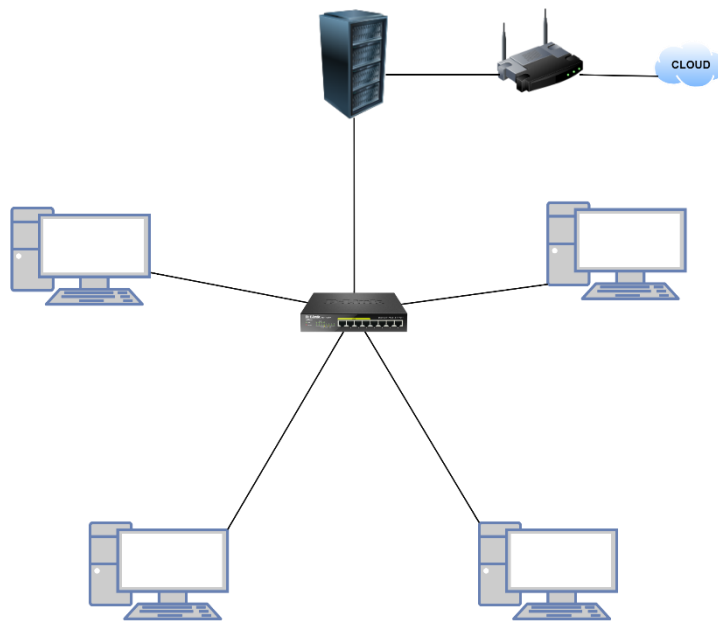
Saran Pengembangan Infrastruktur Jaringan:

- **Menggunakan topologi jaringan syaraf yang lebih kompleks:** jaringan syaraf konvolusional atau jaringan syaraf berulang, untuk meningkatkan akurasi deteksi.
- **Meningkatkan ukuran dataset:** Diperlukan upaya untuk mengumpulkan lebih banyak data serangan brute force untuk melatih model jaringan syaraf. Hal ini dapat meningkatkan generalisasi model dan membuatnya lebih efektif dalam mendeteksi serangan di dunia nyata.
- **Menerapkan model jaringan syaraf secara real-time:** Model jaringan syaraf dapat diimplementasikan secara real-time pada IDS untuk mendeteksi dan mencegah serangan brute force secara langsung.

Topologi Jaringan:

- **Jaringan syaraf konvolusional:** Jaringan syaraf konvolusional dapat digunakan untuk mengekstrak fitur dari data lalu lintas jaringan yang dapat digunakan untuk mengidentifikasi pola serangan brute force.

Topologi STAR



Topologi Berbasis Jaringan Syaraf Konvolusional:

- **Jaringan Inti:**
 - Terdiri dari beberapa layer konvolusional, pooling, dan aktivasi.
 - Setiap layer konvolusional mengekstrak fitur dari data lalu lintas jaringan, menggunakan filter konvolusi.
 - Layer pooling mengurangi dimensi data, meningkatkan efisiensi komputasi.

- Layer aktivasi memperkenalkan non-linearitas pada model, memungkinkan model untuk mempelajari pola yang kompleks.
- **Jaringan Klasifikasi:**
 - Terletak setelah jaringan inti.
 - Terdiri dari beberapa layer fully-connected (FC) dan layer aktivasi.
 - Layer FC menggabungkan fitur yang diekstrak dari jaringan inti.
 - Layer aktivasi memberikan output akhir, mengklasifikasikan data lalu lintas jaringan sebagai normal atau serangan brute force.

Keunggulan Topologi:

- **Efektif dalam mengekstrak fitur:** Jaringan konvolusional mampu mengekstrak fitur spasial dan temporal dari data lalu lintas jaringan, yang penting untuk mendeteksi pola serangan brute force.
- **Robus terhadap variasi data:** Topologi ini dapat menangani variasi data lalu lintas jaringan, seperti perubahan protokol dan pola serangan.
- **Efisiensi komputasi:** Layer pooling membantu mengurangi dimensi data, meningkatkan efisiensi komputasi dan mengurangi kebutuhan memori.
- **Kemampuan klasifikasi:** Jaringan klasifikasi dengan layer FC mampu mengklasifikasikan data lalu lintas jaringan dengan akurasi tinggi.

Alasan Utama Penggunaan Topologi Star

Topologi star menawarkan beberapa keunggulan signifikan dibandingkan topologi jaringan lain, menjadikannya pilihan populer untuk berbagai aplikasi. Berikut beberapa alasan utama mengapa topologi star banyak digunakan:

Kesederhanaan dan Kemudahan Implementasi:

- Topologi star sangat mudah dipahami dan diimplementasikan dibandingkan dengan topologi lain seperti bus atau mesh.
- Kabel terhubung langsung ke perangkat pusat (hub atau switch), memudahkan pengaturan dan troubleshooting.
- Struktur yang sederhana memudahkan penambahan atau penghapusan perangkat tanpa mengganggu jaringan yang ada.

Skalabilitas Tinggi:

- Topologi star dapat diubah skalanya dengan mudah untuk mengakomodasi lebih banyak perangkat dengan menambahkan hub atau switch tambahan.

- Skalabilitas ini membuatnya ideal untuk jaringan yang berkembang atau yang membutuhkan fleksibilitas untuk menambah perangkat di masa depan.

Keandalan dan Ketahanan terhadap Gangguan:

- Jika satu perangkat dalam topologi star gagal, perangkat lain tidak terpengaruh karena mereka terhubung secara independen ke hub atau switch.
- Hal ini meningkatkan keandalan jaringan dan meminimalkan downtime.
- Kerusakan pada hub atau switch dapat memengaruhi semua perangkat yang terhubung, namun jarang terjadi dan mudah diidentifikasi.

Efisiensi dan Pengurangan Tabrakan Data:

- Topologi star meminimalkan tabrakan data karena setiap perangkat berkomunikasi secara langsung dengan hub atau switch, tidak seperti topologi bus di mana semua perangkat berbagi kabel yang sama.
- Hal ini meningkatkan efisiensi jaringan dan meminimalkan latensi (waktu tunggu) data.

Keamanan yang Lebih Baik:

- Topologi star memungkinkan implementasi kontrol akses dan segmentasi jaringan yang lebih mudah, meningkatkan keamanan.
- Setiap perangkat dapat diisolasi dari perangkat lain, membatasi penyebaran malware atau akses yang tidak sah.

Kemudahan Manajemen Jaringan:

- Topologi star memudahkan manajemen jaringan karena perangkat terhubung secara terpusat ke hub atau switch.
- Alat manajemen jaringan dapat digunakan untuk memantau dan mengontrol perangkat secara terpusat.

Kompatibilitas dengan Berbagai Perangkat:

- Topologi star kompatibel dengan berbagai jenis perangkat jaringan, seperti komputer, printer, dan server.
- Hal ini memungkinkan fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan jaringan.

Gambaran dan Saran Pengembangan Infrastruktur Jaringan “Prototype of Automatic Control System for Water Temperature and Acidity in Ornamental Fish Aquarium Based on Internet of Things (IOT)”

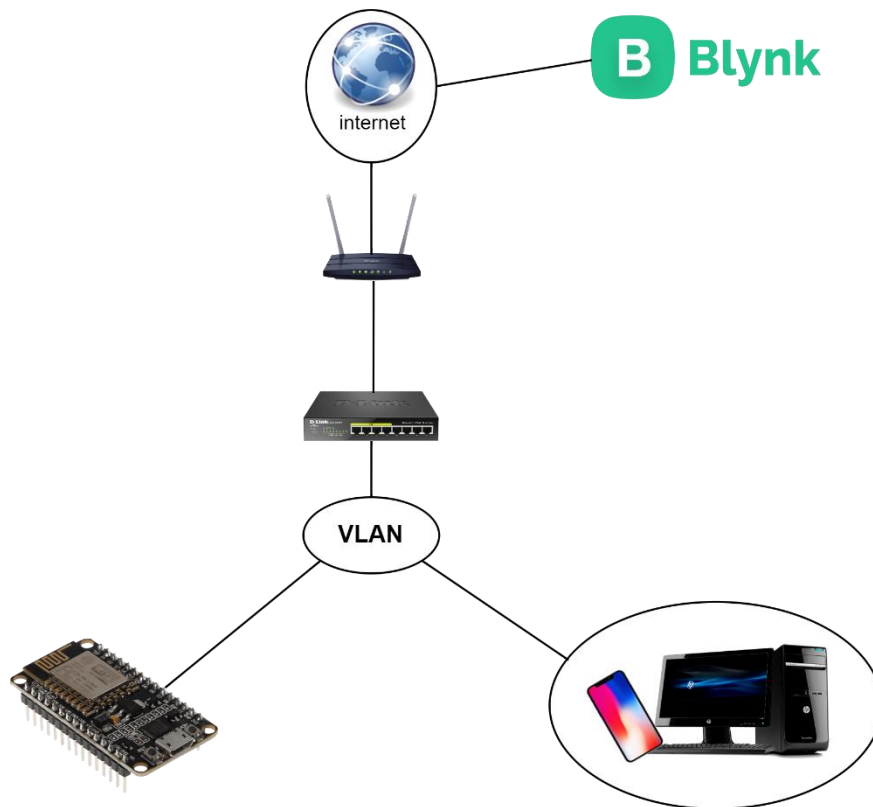
Gambaran:

Jurnal ini memberikan kontribusi yang signifikan dalam pengembangan sistem kontrol otomatis untuk menjaga kondisi air dalam akuarium ikan hias berbasis Internet of Things (IoT). Dengan menggunakan NodeMCU ESP 8266 sebagai mikrokontroler yang terhubung dengan sensor suhu dan pH, alat ini mampu memberikan pemantauan real-time yang akurat terhadap kondisi air dalam akuarium. Hasil pengujian yang dilaporkan menunjukkan kinerja yang baik, dengan suhu rata-rata 28,99 derajat Celsius dan pH 5,44. Desain alat dan metode pengujian yang terperinci memberikan pemahaman yang jelas tentang implementasi sistem ini.

Saran Pengembangan Infrastruktur Jaringan:

Dalam pengembangan infrastruktur jaringan untuk sistem ini, beberapa hal yang perlu dipertimbangkan adalah kestabilan sinyal WiFi, skema keamanan, dan skema pengelolaan data. Berikut adalah topologi jaringan yang disarankan beserta deskripsinya:

Topologi Jaringan:



1. Topologi Star:

- Deskripsi: Setiap perangkat terhubung langsung ke node sentral (router atau switch). NodeMCU ESP 8266, laptop, dan ponsel pintar akan terhubung ke router atau switch melalui koneksi WiFi.
- Saran: Pastikan router atau switch yang digunakan memiliki kapasitas yang cukup untuk menangani lalu lintas data dari semua perangkat terhubung. Selain itu, pastikan sinyal WiFi cukup kuat untuk mencakup area akuarium dan perangkat yang terhubung.

2. Segregasi Jaringan:

- Deskripsi: Pisahkan jaringan IoT (digunakan untuk sistem kontrol akuarium) dari jaringan rumah atau kantor utama. Ini bisa dilakukan dengan menggunakan VLAN (Virtual Local Area Network) atau subnetting.
- Saran: Dengan segregasi jaringan, keamanan sistem dapat ditingkatkan karena akses dari perangkat IoT terbatas hanya pada perangkat dan layanan yang relevan. Hal ini juga membantu mencegah gangguan pada jaringan utama.

3. Pemantauan Jaringan:

- Deskripsi: Implementasikan sistem pemantauan jaringan untuk memantau kesehatan dan kinerja jaringan secara keseluruhan, termasuk konektivitas dan penggunaan bandwidth.
- Saran: Gunakan perangkat lunak pemantauan jaringan seperti Zabbix, Nagios, atau PRTG untuk mendeteksi dan mengatasi masalah jaringan secara proaktif. Ini membantu menjaga ketersediaan sistem secara optimal.

4. **Pengamanan Jaringan:**

- Deskripsi: Terapkan langkah-langkah keamanan yang kuat, termasuk enkripsi data dan autentikasi pengguna untuk mengakses sistem.
- Saran: Gunakan protokol enkripsi seperti WPA2 atau WPA3 untuk melindungi koneksi WiFi. Selain itu, terapkan sandi yang kuat dan autentikasi dua faktor jika memungkinkan untuk mengamankan akses ke aplikasi pengendalian sistem.