Volume 2 (5), 2022

IMPLEMENTASI KEAMANAN IOT MENGGUNAKAN METODE BERLAPIS DALAM BERKOMUNIKASI ANTAR DATA MELALUI JARINGAN SELULER

Yustisio[1*)], Afifudin[2*)]
[1]Teknik Komputer
[2]Teknologi Informasi
*) cinthyabela123@gmail.com

Abstrak

Tujuan dari penelitian ini adalah untuk mengajukan metode berlapis-lapis untuk mengamankan transportasi data dari perangkat Internet of Things yang terhubung seluler ke host melalui jaringan seluler. Metode ini menggunakan banyak elemen keamanan yang saling terkait – yang dijelaskan dalam makalah ini – yang bila diterapkan secara keseluruhan akan memberikan solusi konektivitas yang sangat aman.

Kata Kunci: IOT, Kemanan Berlapis, Komunikasi Data dan Jaringan Seluler.

PENDAHULUAN

Dengan pertumbuhan pesat solusi Internet of Things (IoT), kekhawatiran tentang masalah keamanan terkait dengan banyaknya perangkat yang terhubung semakin meningkat (Riski et al., 2021) (Zanofa et al., 2020). Pertumbuhan perangkat IoT yang terhubung diprediksi akan melebihi 20 miliar perangkat pada tahun 2020 (Rahman Isnain et al., 2021). Banyak dari solusi ini menggunakan dan menggunakan koneksi seluler untuk jaringan. Koneksi seluler yang dirancang dengan buruk dapat membuka potensi masalah keamanan (Nurkholis & Sitanggang, 2019) (Megawaty & Santia, 2019). Solusi arsitektur yang sangat aman memerlukan pendekatan keamanan berlapis yang mencakup seluruh desain arsitektur untuk konektivitas, dari perangkat edge hingga host target untuk pemrosesan, penyimpanan, dan pengiriman selanjutnya (Lukman et al., 2021).

Alternatif untuk konektivitas seluler mencakup solusi yang dapat menggunakan Ethernet atau Wi-Fi nirkabel dan mengandalkan Internet publik untuk mengirimkan data dari perangkat edge ke host (Samsugi et al., 2021) (Rusliyawati & Sinaga, 2017) (Ahdan & Susanto, 2021). Solusi alternatif ini memiliki beberapa kerentanan keamanan. Sifat mandiri dari solusi IoT yaitu Mesin yang berkomunikasi secara mandiri dengan host pendukung yang menurut definisi tidak memerlukan interaksi atau pengawasan manusia, sehingga

memberikan dasar untuk pemantauan jarak jauh dan pelacakan sejumlah solusi IoT yang berguna (Utami et al., 2021) (Surahman et al., 2021). Karena sifat transmisi data, yang tidak terus menerus dipantau atau dimulai oleh input manusia, serangan dapat terjadi tanpa sepengetahuan manusia, seperti perangkat nirkabel portabel yang tidak berfungsi seperti yang diharapkan (Sari & Isnaini, 2021). Faktanya, baru-baru ini, serangan keamanan menggunakan kerentanan terkait Wi-Fi telah muncul melalui Internet publik sebagai cara untuk menyuntikkan aliran data dan mendapatkan kontrol atau aktivitas perangkat IoT (Jupriyadi et al., 2021) (Nani & Ali, 2020).

Metodologi berlapis untuk menyediakan konektivitas nirkabel aman yang dijelaskan di sini menggunakan data agregat yang ditemukan di 3G dan teknologi operator seluler yang lebih tinggi untuk menciptakan koneksi yang kuat antara perangkat IoT dan host pendukung untuk komunikasi dua arah (Ahdan et al., 2020). Metodologi ini terdiri dari sejumlah elemen fungsional yang saling terkait, yang dibahas secara bergantian di seluruh makalah ini. membahas masalah diatas maka peneliti mengangkat judul "Implementasi Keamanan IoT Menggunakan Metode Berlapis Dalam Berkomunikasi Antar Data Melalui Jaringan Seluler".

KAJIAN PUSTAKA

SISTEM ARSITEKTUR

Gambar 1 Sistem Arsitektur

Diagram arsitektur yang sangat disederhanakan yang dijelaskan dalam penelitian ini. Perangkat seluler IoT terhubung ke menara seluler lokal melalui jaringan enkripsi akses radio. Menara lokal terhubung dengan aman ke pusat data mobilitas operator rumah. Host tujuan terhubung melalui tautan terenkripsi titik ke titik.

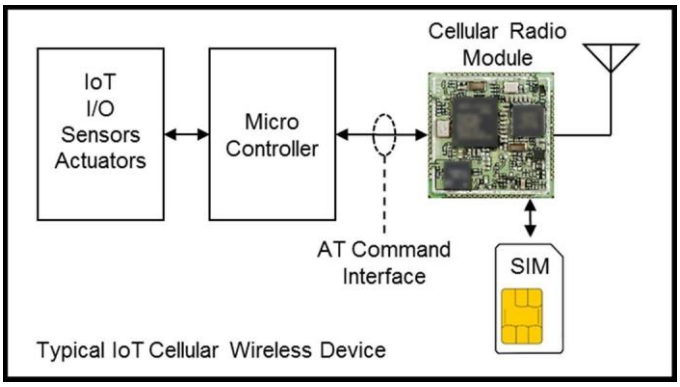
Keuntungan berbeda dari arsitektur ini adalah ia menggunakan elemen berbasis standar yang memungkinkan solusi untuk diterapkan pada perangkat dengan IoT dan keamanan ujung ke ujung, semuanya dicapai tanpa biaya (Rahmanto et al., 2021).

Enkripsi Data Dari Perangkat Ke Host

Mengenkripsi aliran data sebelum meninggalkan edge dan membiarkannya tidak terenkripsi di host memberikan lapisan keamanan ekstra, yang biasanya mengorbankan throughput data yang lebih tinggi yang diukur per bit (Ahmad et al., 2022). Arsitektur yang dijelaskan dalam dokumen ini memberikan keamanan yang diinginkan tanpa meningkatkan biaya enkripsi keamanan data (Pramana et al., 2017) (Wantoro et al., 2021). Untuk banyak kelas aplikasi Internet of Things, solusi ini memungkinkan data TCP atau UDP dikirim dengan jelas, tetapi arsitektur yang aman menyediakan serangkaian elemen fungsional keamanan dasar yang memuaskan yang dapat diintegrasikan dengan benar untuk mencegah akses tidak sah ke saluran data proaktif (Satria & Haryadi, 2018) (Kurniati et al., 2015).

Otentikasi BERBASIS SIM DAN PERJANJIAN KUNCI

Elemen penting pertama dari arsitektur yang aman adalah modul SIM atau pengenalan pengguna (Fadly & Wantoro, 2019). Fungsi utama SIM adalah untuk melindungi kunci otentikasi agar tidak disusupi (Surahman et al., 2014). SIM terdiri dari mikroprosesor yang berisi sejumlah teknologi perlindungan perangkat keras untuk mencegah kompromi melalui degradasi kimia, sinar-X, atau beberapa upaya rekayasa balik. Selanjutnya, teknik perlindungan diterapkan pada pin I/O SIM untuk mencegah anomali paksa eksternal yang membuat SIM rentan terhadap gangguan (Bakri & Darwis, 2021) (Fachri et al., 2015). Misalnya, membuat tegangan yang lebih tinggi atau lebih rendah pada pin TX dan RX mengarah ke suplai dan ground untuk mengunci sirkuit I/O atau memasuki keadaan yang tidak diinginkan di mana sirkuit I/O SIM dikontrol dan kartu SIM berada (Purnomo et al., 2017). SIM juga dilindungi dari pencatatan jam kerja yang tidak wajar dan data masukan (Bakri & Irmayana, 2017). Gambar 2 berikut merupakan komponen dari IoT :



Gambar 2 Komponen IoT

Seperti yang ditunjukkan pada Gambar 2, Sambungan ke kartu SIM dibuat hanya melalui modul seluler, yang mencegah mikroprosesor terintegrasi mengakses kartu SIM secara langsung (Jupriyadi et al., 2020) (Genaldo et al., 2020). Semua komunikasi dengan SIM hanya terjadi melalui lapisan radio yang terpasang di modul radio (Firmansyah et al., 2018).

Ketika perangkat seluler, dalam hal ini perangkat Internet of Things, dinyalakan, radio secara otomatis diprogram untuk memindai pita radio yang tersedia dan membuat katalog. Proses ini diatur untuk memilih menara operator yang pertama-tama cocok dengan kode jaringan seluler (MNC) operatornya sendiri. Ini dilakukan dengan mencari band radio untuk mencari kode siaran yang cocok dengan kode identitas Pelanggan Seluler Internasional (IMSI) SIM. Jika operator yang cocok tidak ditemukan, yaitu operator asal SIM, radio akan memindai operator yang melayani lainnya dan membandingkannya dengan daftar mitra roaming pilihan yang dapat diperbarui. Spesifikasi 3GPP 11.11 menjelaskan mekanisme otentikasi dan pembuatan kunci sandi yang digunakan oleh SIM dan jaringan operator untuk mengotentikasi SIM dan perangkat. Mekanisme otentikasi dan perjanjian kunci yang menggunakan kunci rahasia K yang hanya diketahui oleh SIM dan operator rumah Internet of Things .

METODE

SIM menyediakan metode yang sangat aman untuk mengautentikasi perangkat IoT bahkan sebelum tautan data dibuat. SIM juga berperan dalam beberapa elemen fungsional keamanan lainnya sebagaimana diartikulasikan selanjutnya.

ENKRIPSI JARINGAN AKSES RADIO

Elemen keamanan tambahan sebagai bagian dari keseluruhan metodologi keamanan transmisi data adalah bahwa lapisan tautan radio antara modul radio perangkat IoT dan menara seluler dienkripsi menggunakan kunci bagian sebelumnya sebagai bagian dari GSM 128-bit standar. - protokol. untuk transmisi 3G ke atas (Suri & Puspaningrum, 2020).

NAMA TITIK AKSES KUSTOM (APN)

Setelah perangkat IoT mengautentikasi dengan operator seluler yang melayani, mikroprosesor di perangkat IoT dapat memulai sesi data untuk transmisi TCP/IP. Set perintah adalah perpanjangan dari set perintah modem Hayes alias AT. Mikroprosesor

mengirimkan perintah AT ke radio, melewati variabel tertentu, termasuk nama titik akses (APN) yang ingin dihubungkan oleh aplikasi (Kurniawan et al., 2019). Di telepon konsumen, APN adalah nama umum untuk semua telepon yang digunakan operator rumahan untuk mengirimkan data seluler dan tablet ke internet publik (Nurkholis et al., 2022). Paket data ini biasanya dirutekan melalui terjemahan alamat port (PAT) dan kemudian melalui firewall stateful ke Internet publik. Meskipun praktik umum ini bekerja dengan baik untuk solusi berbasis konsumen, yang memerlukan akses ke Internet yang lebih luas, praktik ini memperkenalkan titik kerentanan keamanan dalam arsitektur Internet of Things.

Arsitektur IoT aman yang disajikan di sini menggunakan APN khusus yang ditetapkan untuk setiap pelanggan perusahaan menggunakan perangkat IoT. APN khusus ini unik untuk perusahaan yang dapat menerapkan dan mengelola perangkat IoT. APN kustom memungkinkan perusahaan tersebut (dan hanya perusahaan tersebut) untuk mengizinkan perangkat IoT mengakses APN kustom perusahaan tersebut untuk mengirimkan data (Syambas et al., 2018).

Menggunakan APN unik khusus menyediakan mekanisme keamanan berikut. Sementara orang yang tidak curiga mungkin dapat menemukan atau menebak nama APN default organisasi, hanya dengan meminta APN melalui perintah AT tidak memungkinkan perangkat tersebut disediakan dan diautentikasi untuk menggunakan APN default tersebut. Mekanisme untuk memastikan bahwa perangkat IoT yang meminta APN khusus diberi wewenang untuk menggunakan APN khusus itu untuk transmisi data didasarkan pada operasi otentikasi yang dijelaskan sebelumnya di Bagian III-A (Sulistiani et al., 2020).

Pada saat ini dalam pembentukan layanan data, elemen yang melayani dalam jaringan home carrier adalah Gateway GPRS Support Node (GGSN) atau Packet Data Network Gateway (PDN-GW). GGSN/PDN-GW bertindak sebagai mediator untuk menetapkan sesi data dan karakteristik melalui koneksi yang membentang dari perangkat IoT melalui jaringan radio ke pusat data mobilitas dan ke dalam elemen GGSN/PDN-GW. Arah keluar dari GGSN/PDN-GW keluar dari pusat data mobilitas juga dipetakan dan dikendalikan oleh parameter dalam konstruksi APN khusus di mana perutean paket data TCP/IP alih-alih pergi ke Internet publik (alias pengalaman konsumen) akan beralih dari pusat data mobilitas keluar melalui koneksi titik ke titik ke host tujuan secara langsung (menerima dan mengumpulkan

data yang disediakan perangkat IoT). Rincian lebih lanjut dapat ditemukan di bagian di bawah ini.

ALAMAT TCP/IP NON-ROUTABLE PRIBADI

Salah satu metodologi aman utama yang digunakan dalam pemilihan dan pengaturan konstruksi APN kustom adalah penggunaan pengalamatan IP pribadi, biasanya rentang kelas B 10.x. GGSN/PDN-GW menetapkan alamat IP kelas B selama koneksi data yang diatur antara modul radio IoT dan pusat data mobilitas. Alamat IP pribadi yang ditetapkan secara dinamis dipilih dari rentang alamat IP yang tersedia seperti yang ditentukan oleh konstruksi APN.

Alamat IP 10.x yang tidak dapat dirutekan yang ditetapkan ke tautan radio disimpan dalam paket di sepanjang jalur antara modul radio IoT dan GGSN/PDN-GW menghindari Terjemahan Alamat Jaringan (NAT) atau Terjemahan Alamat Port (PAT) atau jenis konversi lainnya menjadi alamat IP yang dapat dirutekan publik. Karena sifat arsitektur yang menyeluruh, skema pengalamatan IP pribadi tidak merutekan ke Internet publik. Mengingat sifat pengalamatan IP yang tidak dapat dirutekan yang dipertahankan ujung-ke-ujung, bahkan jika paket berbahaya masuk ke pipa aman ini atau salah satu paket IP "melarikan diri" dari pipa, mereka akan segera dijatuhkan oleh hop router pertama karena alamat IP yang tidak dapat dirutekan. Keamanan inheren yang menyertai skema pengalamatan IP non-routable dan fakta bahwa APN khusus hanya dapat dibuat dan disediakan oleh pelanggan perusahaan yang dituju memberikan solusi yang sangat aman yang mencegah lalu lintas data dicegat atau diinterupsi secara berbahaya.

Penggunaan pengalamatan IP yang tidak dapat dirutekan tidak mencegah aplikasi mengakses informasi yang tersedia melalui Internet publik. Misalnya, perangkat IoT di penyiram air komersial mungkin harus menanyakan sumber informasi eksternal seperti informasi cuaca. Pengontrol IoT dari penyiram air komersial dapat meminta ramalan cuaca untuk menentukan apakah perlu menyiram pada hari tertentu. Paket IP yang dihasilkan oleh mikroprosesor pengontrol IoT sebagai permintaan keluar akan memiliki tujuan URL Administrasi Kelautan dan Atmosfer Nasional (NOAA) yang menyediakan umpan cuaca yang dapat dibaca mesin. Arsitektur skema aman seperti yang diartikulasikan dalam makalah ini akan mengirimkan paket yang ditujukan kepada tujuan publik melalui sistem ke router

pelanggan di pusat data mereka. Paket beralamat IP publik itu kemudian dapat diproksikan ke Internet publik setelah melewati router dan firewall pelanggan perusahaan.

SKEMA ROUTING TEROWONGAN NON-SPLIT

Solusi yang dirancang dengan buruk sering kali menyediakan APN untuk terowongan bersama. Dengan kata lain, Sementara paket 10.x yang berisi data pribadi dikirim langsung ke klien perusahaan seperti yang dijelaskan sebelumnya, paket yang menghadap publik dikirim langsung ke klien perusahaan (Ramadona et al., 2021). dipindahkan dari pusat data seluler ke Internet publik. Meskipun ini adalah arsitektur yang didukung, ini merusak metodologi keamanan karena perangkat IoT sekarang memiliki akses ke internet publik yang tidak berada di bawah kendali pelanggan perusahaan (Ahdan et al., 2019).

TRANSPORT DATA POINT TO POINT ANTARA CARRIER SELULER DAN HOST

Koneksi point-to-point antara pusat data mobilitas dan host tujuan dapat berbentuk terowongan IPsec VPN, atau MPLS, atau frame relay, atau sejumlah solusi konektivitas point-to-point aman darat yang mungkin ditawarkan oleh sisi keluar dari layanan pengangkut. Yang paling umum adalah IPsec VPN yang umumnya menggunakan peralatan Cisco firewall VPN di kedua operator dan situs data host. Dengan menggabungkan dua elemen fungsional yang disediakan oleh terowongan APN dan IPsec VPN khusus, dimungkinkan untuk membuat pipa aman tertutup mulai dari modul radio di dalam perangkat IoT sampai ke menara dan pusat data mobilitas operator yang transit melalui GGSN /PDN-GW, disalurkan melalui pusat data mobilitas melalui pipa aman off-the-Internet khusus ke host pelanggan perusahaan yang berakhir di router IPsec VPN (Sulistiani et al., 2020).

TIDAK ADA KOMUNIKASI PERANGKAT LANGSUNG KE PERANGKAT

Menariknya, istilah yang sering digunakan untuk IoT adalah machine-to-machine (M2M), yang mengarah pada kesalahpahaman bahwa perangkat IoT berkomunikasi secara langsung satu sama lain. Metodologi yang dijelaskan dalam dokumen ini melarang komunikasi perangkat-ke-perangkat langsung melalui operator klien atau router host (Sulistiani et al., 2019). Faktanya, komunikasi perangkat IoT hanya diarahkan ke lapisan aplikasi yang

mengelola solusi IoT dalam host backend. Jika solusi memerlukan dan pertukaran data antara perangkat IoT A dan perangkat IoT B, tujuan ini dicapai melalui lapisan aplikasi di server host backend, sebagai lawan dari pertukaran paket data langsung antara kedua perangkat. Meskipun secara teknis dimungkinkan untuk mengonfigurasi APN ke perutean perangkat-ke-perangkat 'menjepit rambut' melalui pusat data operator, pendekatan ini merusak metodologi keamanan yang dijelaskan di sini. Jika perangkat IoT diizinkan untuk berkomunikasi secara langsung satu sama lain melalui pusat data operator, prosedur ini tidak akan meninggalkan catatan atau jejak di router pelanggan atau sistem host backend. Dengan kata lain, perangkat mungkin mengobrol bolak-balik tanpa pelanggan perusahaan memiliki catatan atau melihat lalu lintas perangkat M2M, sehingga tidak dapat menyelidiki lalu lintas untuk perilaku jahat.

PEMANTAUAN ROUTER HOST TUJUAN

Manfaat tidak berwujud lainnya dari perutean aman ini adalah bahwa semua paket data ke perangkat IoT melewati router pelanggan perusahaan. Inspeksi paket mendalam pada router pelanggan dapat mendeteksi secara real-time ketika perilaku data abnormal terjadi dari perangkat IoT, yang dapat mengindikasikan aktivitas penipuan atau berbahaya (Yunitasari & Sintaro, 2021). Alarm otomatis kemudian digunakan untuk memicu sistem penyediaan untuk menonaktifkan perangkat IoT dan memperingatkan intervensi teknis. Ini tidak mungkin jika paket data yang dirutekan secara publik di-tunnel di situs operator dan hanya paket dengan 10.x yang akan melewati router perusahaan pelanggan. Dengan mengirimkan setiap paket melalui router perusahaan pelanggan, pusat data host pelanggan memiliki pandangan holistik dari semua lalu lintas yang datang dan pergi ke perangkat IoT dan secara forensik dapat mendeteksi apakah perilaku curang sedang atau telah terjadi.

VALIDASI DAN PEMBERITAHUAN SIM TOOLKIT IMEI

salah satu bentuk perlindungan fisik. Salah satu metode yang dijelaskan adalah bahwa setelah perangkat IoT membuat koneksi aman antara radionya dan host yang melayani backend, keamanan tambahan disediakan dalam keamanan perangkat keras fisik yang tertanam dalam elemen SIM untuk melindungi kunci terenkripsi yang tercakup dalam perlindungannya. Fitur perangkat keras kedua adalah nomor seri unik yang terdapat pada chipset radio. Ini disebut sebagai IMEI atau International Mobile Equipment Identifier

(Mastra & Dharmawan, 2018). Setiap pabrikan perangkat nirkabel, setelah mengisi kode pabrikan/produk yang disebut sebagai kode jenis penugasan (TAC). Oleh karena itu IMEI mampu mengidentifikasi hingga satu juta perangkat unik. Nomor IMEI ini terdaftar dalam database yang dapat dicari untuk anggota badan PTCRB. Operator pengujian persetujuan PTCRB yang diperlukan diberi rentang IMEI yang unik untuk produknya. Nomor seri IMEI panjangnya 15 digit (16 dalam versi perangkat lunak IMEI), dengan enam digit berisi nomor seri unik dan delapan digit sebelumnya mengidentifikasi seluler dapat dengan mudah mengidentifikasi merek dan model perangkat IoT dari kode IMEI unik yang disimpan di dalam chipset radio. Bagian dari catatan yang dipertukarkan antara modul radio perangkat IoT dan operator yang melayani selama otentikasi adalah pemasangan IMEI dan International Mobile Subscriber Identity (IMSI), yang merupakan nomor seri SIM. Operator dapat menggunakan kedua kode untuk mengautentikasi, mengizinkan, atau menolak layanan konektivitas jika perilaku curang terdeteksi dengan salah satu elemen ini, dan menentukan apakah perangkat tersebut merupakan perangkat tepercaya yang telah menjalani sertifikasi ketat oleh operator dan industri untuk mencapai IMEI uniknya. urutan kode.

Ada lagi fitur keamanan unik yang ditawarkan oleh SIM. Menjadi mikroprosesor tersendiri, yang memiliki ruang kode yang dapat dieksekusi, SIM menjalankan serangkaian program mekanisme keamanan yang hanya diketahui oleh operator. Metodologi dalam makalah ini menjelaskan urutan dalam pemrograman SIM yang saat dihidupkan meminta IMEI dari modul radio yang terhubung langsung. SIM yang menjadi lokasi penyimpanan aman telah menerima salinan IMEI perangkat terhubung yang diizinkan atau menemukannya saat pertama kali dihidupkan. IMEI yang diizinkan ini disimpan dalam memori non-volatil di dalam SIM dan setelah dihidupkan, SIM membuat dimaksudkan untuk masuk karena nomor seri peralatan cocok dengan nomor seri perangkat keras yang diizinkan dan disimpan dengan aman.

PENGUNCI PIN SIM

Fungsi kunci PIN SIM standar digunakan oleh perangkat IoT sebagai metode keamanan. Pabrikan perangkat keras membuat algoritme hashing yang aman pada CPU perangkat yang dikunci oleh nomor seri perangkat keras, mis. B. IMEI, yang membuat nomor digit unik. Saat terhubung, kartu SIM yang terkait dengan perangkat diprogram ke mode terkunci dengan kode unik digit sebagai kunci (Aji & Dewi, 2017). Selama aktivasi atau reset, SIM

meminta kode buka kunci melalui antarmuka udara ke prosesor perangkat . Firmware menjalankan algoritma hashing untuk menghasilkan kode buka kunci 4 digit dan lolos ke SIM. Jika kode cocok dengan SIM maka SIM diaktifkan untuk operasi. Jika pin tidak cocok setelah 3 kali percobaan, SIM menjadi tidak dapat digunakan atau diblokir. Solusi ini mencegah SIM dikeluarkan dari perangkat IoT dan dimasukkan ke telepon konsumen. UI telepon akan meminta pin yang tidak akan diketahui orang jahat dan hanya setelah 3 kali gagal, SIM tidak lagi berfungsi. Ada urutan pembukaan blokir menggunakan kode 8 digit yang hanya diketahui oleh penyedia perangkat yang dapat membuka blokir SIM dan jika itu salah diberikan 10 kali, SIM menjadi tidak dapat dioperasikan secara permanen .

SIMPULAN

Penelitian ini telah menetapkan solusi multi-tingkat untuk secara aman membangun komunikasi Internet of Things berbasis TCP/IP ujung-ke-ujung melalui jaringan berbasis seluler UMTS/LTE. Metodologi ini terdiri dari elemen fungsional interlocking berbasis standar yang digunakan dalam jaringan operator yang dirancang dengan aman yang menyediakan saluran komunikasi ujung ke ujung yang aman untuk perangkat dan aplikasi Internet of Things

REFERENSI

Ahdan, S., Kaharuddin, A. H. B., & Yusriadi Yusriadi, U. F. (2019). Innovation And Empowerment Of Fishermen Communities In Maros Regency. *International Journal of Scientific and Technology Research*, *8*(12).

Ahdan, S., Putri, A. R., & Sucipto, A. (2020). Aplikasi M-Learning Sebagai Media Pembelajaran Conversation Pada Homey English. *Sistemasi*, *9*(3), 493. https://doi.org/10.32520/stmsi.v9i3.884

Ahdan, S., & Susanto, E. R. (2021). IMPLEMENTASI DASHBOARD SMART ENERGY UNTUK PENGONTROLAN RUMAH PINTAR PADA PERANGKAT BERGERAK BERBASIS INTERNET OF THINGS. *Jurnal Teknoinfo*, *15*(1), 26–31.

Ahmad, I., Febrian, A., & Prastowo, A. T. (2022). *PENERAPAN DAN PENDAMPINGAN SISTEM TRACER STUDY SECARA ONLINE PADA MA MA ’ ARIF 1 PUNGGUR*. *3*(1), 277–282.

Aji, G. F. S., & Dewi, N. (2017). Prosiding Seminar Nasional: Membongkar Sastra, Menggugat Rezim Kepastian. In *Prosiding Seminar Nasional: Membongkar Sastra, Menggugat Rezim Kepastian*.

Bakri, M., & Darwis, D. (2021). *PENGUKUR TINGGI BADAN DIGITAL ULTRASONIK BERBASIS ARDUINO DENGAN LCD DAN OUTPUT*. *2*, 1–14.

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. *Jurnal Tekno Kompak*, *11*(2), 41–44.

Fachri, M. R., Sara, I. D., & Away, Y. (2015). Pemantauan Parameter Panel Surya Berbasis

Arduino secara Real Time. *Jurnal Rekayasa Elektrika*, *11*(4), 123. https://doi.org/10.17529/jre.v11i3.2356

Fadly, M., & Wantoro, A. (2019). Model Sistem Informasi Manajemen Hubungan Pelanggan Dengan Kombinasi Pengelolaan Digital Asset Untuk Meningkatkan Jumlah Pelanggan. *Prosiding Seminar Nasional Darmajaya*, *1*, 46–55.

Firmansyah, M. A., Mulyana, D., Karlinah, S., & Sumartias, S. (2018). Kontestasi Pesan Politik dalam Kampanye Pilpres 2014 di Twitter: Dari Kultwit Hingga Twitwar. *Jurnal Ilmu Komunikasi*, *16*(1), 42. https://doi.org/10.31315/jik.v16i1.2681

Genaldo, R., Septyawan, T., Surahman, A., & Prasetyawan, P. (2020). Sistem Keamanan Pada Ruangan Pribadi Menggunakan Mikrokontroler Arduino dan SMS Gateway. *Jurnal Teknik Dan Sistem Komputer*, *1*(2), 13–19.

Jupriyadi, J., Hijriyanto, B., & Ulum, F. (2021). Komparasi Mod Evasive dan DDoS Deflate Untuk Mitigasi Serangan Slow Post. *Techno. Com*, *20*(1), 59–68.

Jupriyadi, J., Putra, D. P., & Ahdan, S. (2020). Analisis Keamanan Voice Over Internet Protocol (VOIP) Menggunakan PPTP dan ZRTP. *Jurnal VOI (Voice Of Informatics)*, *9*(2).

Kurniati, I. D., Setiawan, R., Rohmani, A., Lahdji, A., Tajally, A., Ratnaningrum, K., Basuki, R., Reviewer, S., & Wahab, Z. (2015). *Buku Ajar Basis Data*.

Kurniawan, D. E., Iqbal, M., Friadi, J., Borman, R. I., & Rinaldi, R. (2019). Smart Monitoring Temperature and Humidity of the Room Server Using Raspberry Pi and Whatsapp Notifications. *Journal of Physics: Conference Series*, *1351*(1). https://doi.org/10.1088/1742-6596/1351/1/012006

Lukman, A., Hakim, A., Maulana, I., Wafa, I., & Koswara, Y. (2021). *Perancangan Aplikasi Inventaris Gudang Menggunakan Bahasa Program PHP dan Database MySQL Berbasis WEB*. *4*(1), 7–13. https://doi.org/10.32493/jtsi.v4i1.7754

Mastra, K. N. L., & Dharmawan, R. F. (2018). Tinjauan User Interface Design Pada Website E-Commerce Laku6. *Narada*, *5*(1), 83–94.

Megawaty, D. A., & Santia, D. (2019). Assessment of The Alignment Maturity Level of Business and Information Technology at CV Jaya Technology. *2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 54–58.

Nani, D. A., & Ali, S. (2020). Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local GovernmeNani, D. A., & Ali, S. (2020). Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local Governments. Jurnal Dinamika Akuntansi. *Jurnal Dinamika Akuntansi Dan Bisnis*, *7*(1), 33–50. https://doi.org/10.24815/jdab.v7i1.15671

Nurkholis, A., Anggela, Y., & Octaviansyah P, A. F. (2022). Web-Based Geographic Information System for Lampung Gift Store. *Jurnal Teknoinfo*, *16*(1), 34. https://doi.org/10.33365/jti.v16i1.1486

Nurkholis, A., & Sitanggang, I. S. (2019). *A spatial analysis of soybean land suitability using spatial decision tree algorithm*. *December*, 65. https://doi.org/10.1117/12.2541555

Pramana, D., Nugraha, D. P., & Prasetya, H. (2017). Alat Teknologi Pendeteksi dan Pembasmi Hama Wereng Berbasis Smartphone. *Jurnal Scientific Pinisi*, *3*(2), 93–97. https://ojs.unm.ac.id/pinisi/article/view/4778

Purnomo, D., Irawan, B., & Brianorman, Y. (2017). Sistem Pakar Diagnosa Penyakit Pada Kucing Menggunakan Metode Dempster-Shafer Berbasis Android. *Jurnal Coding Sistem Komputer Untan*, *05*(1), 23–32.

Rahman Isnain, A., Pasha, D., & Sintaro, S. (2021). Workshop Digital Marketing "Temukan Teknik Pemasaran Secara Daring." *Journal of Social Sciences and Technology for*

Community Service (JSSTCS), *2*(2), 113–120. https://ejurnal.teknokrat.ac.id/index.php/JSSTCS/article/view/1365

Rahmanto, Y., Burlian, A., & Samsugi, S. (2021). SISTEM KENDALI OTOMATIS PADA AKUAPONIK BERBASIS MIKROKONTROLER ARDUINO UNO R3. *Jurnal Teknologi Dan Sistem Tertanam*, *2*(1), 1–6.

Ramadona, S., Diono, M., Susantok, M., & Ahdan, S. (2021). Indoor location tracking pegawai berbasis Android menggunakan algoritma k-nearest neighbor. *JITEL (Jurnal Ilmiah Telekomunikasi, Elektronika, Dan Listrik Tenaga)*, *1*(1), 51–58. https://doi.org/10.35313/jitel.v1.i1.2021.51-58

Riski, M., Alawiyah, A., Bakri, M., & Putri, N. U. (2021). Alat Penjaga Kestabilan Suhu Pada Tumbuhan Jamur Tiram Putih Menggunakan Arduino UNO R3. *Jurnal Teknik Dan Sistem Komputer*, *2*(1), 67–79.

Rusliyawati, & Sinaga, I. (2017). Pengaruh Self-Efficacy Komputer Jurusan Sia (Studi Kasus Mahasiswa Bidang Keahlian Sia Stmik Teknokrat Lampung). *Prosiding Seminar Nasional Darmajaya*, *1*(1), 56–89. https://jurnal.darmajaya.ac.id/index.php/PSND/article/view/750%0Ahttps://jurnal.darmajaya.ac.id/index.php/PSND/article/viewFile/750/484

Samsugi, S., Nurkholis, A., Permatasari, B., Candra, A., & Prasetyo, A. B. (2021). Internet of Things Untuk Peningkatan Pengetahuan Teknologi Bagi Siswa. *Journal of Technology and Social for Community Service (JTSCS)*, *2*(2), 174.

Sari, R. K., & Isnaini, F. (2021). PERANCANGAN SISTEM MONITORING PERSEDIAAN STOK ES KRIM CAMPINA PADA PT YUNIKAR JAYA SAKTI. *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *2*(1), 151–159.

Satria, M. N. D., & Haryadi, S. (2018). Effect of the content store size to the performance of named data networking: Case study on Palapa Ring topology. *Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/TSSA.2017.8272911

Sulistiani, H., Muludi, K., & Syarif, A. (2019). Implementation of Dynamic Mutual Information and Support Vector Machine for Customer Loyalty Classification. *Journal of Physics: Conference Series*, *1338*(1). https://doi.org/10.1088/1742-6596/1338/1/012050

Sulistiani, H., Rahmanto, Y., Dwi Putra, A., & Bagus Fahrizqi, E. (2020). Penerapan Sistem Pembelajaran Dalam Jaringan Untuk Meningkatkan Kualitas Belajar Dalam Menghasilkan Siswa 4.0. *Journal of Technology and Social for Community Service (JTSCS)*, *2*(2), 178–183. https://ejurnal.teknokrat.ac.id/index.php/teknoabdimas

Surahman, A., Aditama, B., Bakri, M., & Rasna, R. (2021). Sistem Pakan Ayam Otomatis Berbasis Internet Of Things. *Jurnal Teknologi Dan Sistem Tertanam*, *2*(1), 13–20.

Surahman, A., Prastowo, A. T., & Aziz, L. A. (2014). *RANCANG ALAT KEAMANAN SEPEDA MOTOR HONDA BEAT BERBASIS SIM GSM MENGGUNAKAN METODE RANCANG BANGUN*.

Suri, M. I., & Puspaningrum, A. S. (2020). Sistem Informasi Manajemen Berita Berbasis Web. *Jurnal Teknologi Dan Sistem Informasi (JTSI)*, *1*(1), 8–14. http://jim.teknokrat.ac.id/index.php/sisteminformasi

Syambas, N. R., Tatimma, H., Mustafa, A., & Pratama, F. (2018). Performance comparison of named data and IP-based network—Case study on the Indonesia higher education network. *Journal of Communications*, *13*(10), 612–617. https://doi.org/10.12720/jcm.13.10.612-617

Utami, A. R., Oktaviani, L., & Emaliana, I. (2021). The Use of Video for Distance Learning During Covid-19 Pandemic: Students' Voice. *Jet Adi Buana*, *6*(02), 153–161.

https://doi.org/10.36456/jet.v6.n02.2021.4047

Wantoro, A., Rusliyawati, R., & Wantoro, A. (2021). *Model sistem pendukung keputusan menggunakan FIS Mamdani untuk penentuan tekanan udara ban Decision support system model using FIS Mamdani for determining tire*. *9*(November 2020), 56–63. https://doi.org/10.14710/jtsiskom.2020.13776

Yunitasari, Y., & Sintaro, S. (2021). *Penggerak Kamera Dengan 2in1 Control (Manual Dan Otomatis) Menggunakan Aplikasi Android*. *02*(02).

Zanofa, A. P., Arrahman, R., Bakri, M., & Budiman, A. (2020). Pintu Gerbang Otomatis Berbasis Mikrokontroler Arduino UNO R3. *Jurnal Teknik Dan Sistem Komputer*, *1*(1), 22–27.