Analisis Proses Akuisisi Data Dari Xiaomi Smart Band 8 Active Dengan Protokol Komunikasi Bluetooth Low Energy

M A Firdaus[1], R R Mardi Putri[*2], R Primananda[3]

[1]PT HiThink Technology Indonesia

[2]Universitas Brawijaya, Indonesia

[3]Universitas Brawijaya Indonesia

E-mail: muhammad.firdaus@dhc.com.cn[1], rekyan.rmp@ub.ac.id[*2], rakhmadhany@ub.ac.id[3]

Abstrak. Teknologi *wearable*, khususnya *smartwatch* dan *smartband*, semakin banyak dimanfaatkan untuk memperoleh data biologis secara non-intrusif. Dibandingkan *smartwatch*, *smartband* memiliki keunggulan dalam efisiensi penggunaan daya, tetapi pemanfaatannya sebagai perangkat akuisisi data primer penelitian masih terbatas. Penelitian ini bertujuan menganalisis metode akuisisi data pada Xiaomi Smart Band 8 Active melalui layanan sinkronisasi berbasis profil GATT. Akuisisi dilakukan menggunakan metode *fingerprinting* untuk menangkap data yang dikirimkan selama proses sinkronisasi. Eksperimen replikasi data yang dikirimkan oleh aplikasi Mi Fitness ke perangkat lain hanya berhasil memperoleh dua frame data. Hal ini diduga terkait dengan adanya mekanisme keamanan pada frame berikutnya yang bergantung pada kedua frame awal, seperti kemungkinan penggunaan enkripsi atau hal lain seperti session token atau sequence counter, namun mengindikasikan kemungkinan enkripsi. Untuk itu perlu dilakukan verifikasi dengan . analisis frekuensi dan entropi terhadap data pada log sinkronisasi. Hasil analisis menunjukkan bahwa distribusi byte pada setiap log tidak bersifat uniform berdasarkan Chi-Squared Goodness-of-Fit Test. Entropi setiap log relatif rendah, dengan rata-rata 1,03 (12,9%) pada data request dan 1,49 (18,6%) pada data response dari entropi maksimum, sedangkan ketika seluruh log digabungkan, entropi mencapai 7,91 (98,9%) pada request dan 7,98 (99,7%) pada response.. Temuan ini mengindikasikan adanya perbedaan karakteristik antarlog dan kemungkinan penerapan enkripsi secara parsial pada data sinkronisasi. Berbeda dengan penelitian terdahulu yang hanya berfokus pada stabilitas profil GATT, penelitian ini memberikan kontribusi berupa identifikasi struktur data BLE secara rinci serta metode akuisisi data di luar aplikasi bawaan pada perangkat smartband

Kata kunci: *wearables; smartbands; Bluetooth Low Energy; GATT; fingerprinting*

Abstract. Wearable technologies, particularly smartwatches and smart-bands, have increasingly been utilized to acquire biological data in a non-invasive manner. Compared with smartwatches, smart-bands offer greater power efficiency; however, their use as primary data acquisition devices in research remains limited. This study investigates a data acquisition method for the Xiaomi Smart Band 8 Active through its synchronization service based on the Generic Attribute Profile (GATT). Data acquisition was performed using a fingerprinting approach to capture data transmitted during the synchronization process. An experiment to replicate data transmitted by the Mi Fitness application to another device successfully captured only two data frames. This is suspected to be linked to a security mechanism in the subsequent frame that relies on the two initial frames—such as the potential use of encryption or other

elements like session tokens or sequence counters—though it points to the possibility of encryption.. Frequency and entropy analyses were subsequently conducted on the synchronization log data to verify the indication of encryption. The results indicate that the byte distribution within individual logs is non-uniform, as confirmed by the Chi-Squared Goodness-of-Fit Test. The entropy of individual logs was relatively low, averaging 1.03 (12.9%) for request data and 1.49 (18.6%) for response data relative to the maximum entropy, whereas the combined logs exhibited an entropy of 7.91 (98.9%) for request and 7.98 (99.7%) for response. These findings indicate significant differences in the characteristics of individual synchronization logs and suggest that the transmitted data may employ partial encryption. Unlike prior work that focused only on GATT profile stability, this study contributes a detailed identification of the BLE data structure and a data acquisition method independent of the vendor's native application.

Keywords: wearables; smartbands; Bluetooth Low Energy; GATT; fingerprinting

1. Pendahuluan

Teknologi wearable adalah perangkat elektronik yang dirancang untuk dikenakan atau diintegrasikan ke tubuh manusia. Perangkat ini populer di bidang kesehatan dan kebugaran karena manfaatnya yang beragam, seperti harga terjangkau, kenyamanan, dan kemampuannya melakukan pengecekan data biologis secara nonintrusif (Thompson, 2022; Huhn et al., 2022). Dengan memanfaatkan sensor, komunikasi nirkabel , wearable memungkinkan pemantauan kesehatan real-time yang dapat dipersonalisasikan sesuai kebutuhan pengguna, membuka peluang untuk pencegahan dan deteksi penyakit kronis (Guk et al., 2019).

Perangkat *wrist-wear* seperti *smartwatch* dan *smartband* dilengkapi berbagai fitur, seperti pengukuran detak jantung, saturasi oksigen, kalori yang terbakar, dan aktivitas gerak. Sensor seperti *photoplethysmography (PPG)* dan akselerometer mendukung beberapa fitur ini, sementara data dikirimkan ke aplikasi melalui protokol seperti *Bluetooth Low Energy (BLE)*. Penelitian sebelumnya juga menunjukkan potensi *wrist-wear* untuk fungsi tambahan, seperti pendeteksian aktivitas selama menyetir (R. R. Mardi Putri et al., 2024) atau selama aktivitas sehari-hari (Mekruksavanich et al., 2020), meski penggunaannya pada smartwatch yang kurang efisien karena konsumsi baterai yang lebih besar. *Smartband* dianggap lebih hemat energi dibandingkan smartwatch karena tidak menggunakan sistem operasi berbasis Android seperti WearOS, yang membutuhkan lebih banyak proses. Sebagai contoh, Xiaomi Smart Band 8 Active hanya membutuhkan baterai 210mAh dan mampu bertahan hingga 14 hari, jauh lebih lama dibandingkan smartwatch seperti Xiaomi Watch 2 Pro dengan 495mAh yang hanya bertahan sekitar 3 hari. Efisiensi ini menjadikan *smartband* lebih ideal untuk pemantauan data biologis dengan daya rendah dan lebih sedikit proses.

Penelitian sebelumnya pada perangkat BLE menunjukkan bahwa fingerprint dari profil Generic Attribute (GATT) dapat digunakan untuk melacak perangkat dan menyimpulkan informasi seperti model perangkat dan data biologis pengguna (Celosia et al., 2019). Namun penelitian ini hanya menganalisis stabilitas profil GATT tanpa mengidentifikasi alur komunikasi atau struktur data yang ditransmisikan. Oleh karena itu, penelitian lebih lanjut diperlukan untuk memahami komunikasi antara perangkat BLE seperti smartband dan aplikasi.

Penelitian ini bertujuan menganalisis komunikasi Xiaomi Smart Band 8 Active dengan aplikasi Android melalui protokol BLE, termasuk alur pengiriman data, struktur data, dan metode akuisisi data di luar aplikasi bawaan. BLE dipilih karena konsumsi dayanya yang rendah dan umum digunakan pada perangkat wearable (Liu et al., 2021). Dengan penelitian ini, diharapkan dapat diperoleh wawasan baru tentang mekanisme komunikasi perangkat wearable terutama penggunaan smartband, sehingga membuka peluang pengembangan aplikasi kesehatan yang lebih efisien dan hemat energi menggunakan perangkat yang telah diproduksi secara massal.er, dan nomor halaman pada naskah Anda karena akan ditambahkan pada saat proses produksi IJIS.

Dibandingkan dengan penelitian sebelumnya yang menganalisis fingerprinting profil GATT pada perangkat BLE namun terbatas pada evaluasi stabilitas profil tanpa mengidentifikasi struktur maupun alur komunikasi data (Celosia & Cunche, 2019), penelitian ini memberikan tiga kontribusi

utama. Pertama, penelitian ini mengidentifikasi struktur frame dan payload BLE pada Xiaomi Smart Band 8 Active secara rinci, termasuk skema data utuh dan data fragmen, yang belum pernah dipublikasikan sebelumnya. Kedua, penelitian ini mengusulkan metode akuisisi data melalui fingerprinting pada services profil GATT tanpa bergantung pada aplikasi bawaan (Mi Fitness), sehingga membuka peluang pemanfaatan data wearable di luar ekosistem aplikasi resmi. Ketiga, penelitian ini menerapkan kombinasi analisis frekuensi dan entropi sebagai indikator awal untuk menduga adanya penerapan enkripsi parsial pada data sinkronisasi perangkat smartband konsumer, suatu pendekatan yang belum diterapkan pada perangkat Xiaomi Smart Band 8 Active.

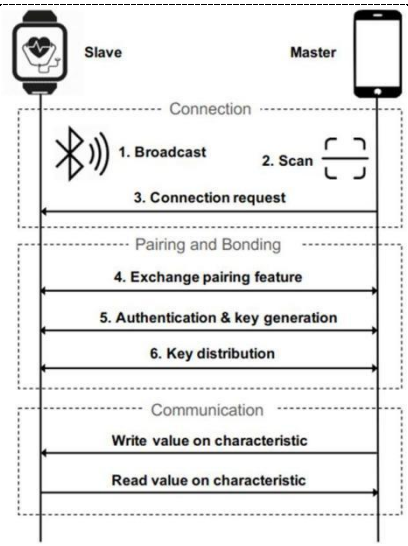
2. Landasan Kepustakaan

2.1. Internet Of Things

Internet of Things (IoT) adalah teknologi yang memungkinkan perangkat saling berkomunikasi dan bertukar informasi melalui jaringan internet tanpa memerlukan interaksi manusia secara langsung. IoT memiliki aplikasi luas di berbagai sektor, seperti pendidikan, industri, smart city, dan kesehatan, dengan manfaat seperti peningkatan efisiensi, otomatisasi proses, dan analisis data real-time (Pradhan et al., 2021). Salah satu penerapan IoT yang menonjol di sektor kesehatan adalah perangkat wearable, seperti smartwatch dan smartband, yang digunakan untuk memantau data kesehatan secara real-time, seperti detak jantung, aktivitas fisik, dan kualitas tidur. Wearables mendukung pemantauan pasien, deteksi dini kondisi kritis, serta personalisasi perawatan melalui integrasi data berbasis cloud (Akkaş et al., 2020). Dengan perkembangan pesat, jumlah perangkat IoT global diproyeksikan mencapai 75 miliar pada 2025 dan 134 miliar pada 2030 (Silva-Trujillo et al., 2023).

2.2. Bluetooth Low Energy

Bluetooth Low Energy atau yang biasa dikenal dengan BLE merupakan variasi dari protokol Bluetooth yang ditujukan untuk menekan tingkat penggunaan daya perangkat dengan menkondisikan untuk berada pada kondisi sleep mode selama tidak ada inisiasi transmisi data (Liu et al., 2024). BLE mulanya dikembangkan berdasarkan versi Bluetooth 4.0 yang kemudian diperbaharui pada versi 4.1 dan 4.2.



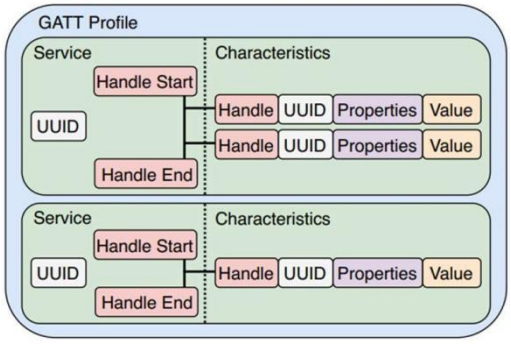
Gambar 1. Alur transmisi pada BLE (Zuo et al., 2019)

Gambar 1 menunjukkan alur komunikasi Bluetooth Low Energy (BLE) antara perangkat slave seperti smartband, dan perangkat master, seperti ponsel pintar. Proses dimulai dengan Fase Koneksi, di mana perangkat slave memancarkan paket iklan untuk ditemukan oleh perangkat master, yang kemudian mengirimkan permintaan koneksi. Dilanjutkan dengan fase pairing dan bonding, kedua

perangkat bertukar informasi dan melakukan autentikasi untuk menghasilkan kunci enkripsi. Pada fase komunikasi, data ditransmisikan dengan perangkat master membaca atau menulis nilai pada characteristic perangkat slave. BLE menjadi protokol komunikasi IoT yang ideal, terutama untuk perangkat wearable, karena mendukung transmisi data dengan efisiensi daya tinggi pada perangkat berukuran kecil (Silva-Trujillo et al., 2023), meski dengan jarak propagasi yang pendek (Liu et al., 2021).

2.3. Attribute Protocol

Attribute Protocol (ATT) dalam BLE adalah protokol stateless berbasis atribut yang dimiliki oleh perangkat di mana setiap perangkat dapat mengadopsi peran tertentu seperti klien atau server terlepas dari peran dalam komunikasi BLE (Celosia et al, 2019). Data yang diekspos oleh server disajikan dalam Generic Attribute Profile (GATT) yang merupakan struktur hierarkis atribut yang memungkinkan transfer informasi antara klien dan server. Dalam profil GATT, atribut dapat berupa layanan atau karakteristik dan diidentifikasi oleh pengenal unik universal (UUID). Dalam struktur hierarkis, karakteristik yang secara konseptual terkait dikelompokkan di bawah layanan yang sama. Contoh struktur hierarkis dapat dilihat pada Gambar 2.



Gambar 2. Struktur hierarkis profil GATT (Celosia et al, 2019)

Dalam profil GATT, characteristics terdiri dari tiga elemen utama yaitu attribute handle, properties, dan value. Attribute handle berfungsi sebagai penunjuk atau pengidentifikasi unik yang menunjukkan lokasi characteristic dalam profil GATT, memungkinkan perangkat untuk mengakses data yang tersimpan. Properties menggambarkan metadata yang menjelaskan jenis operasi yang dapat dilakukan pada characteristic tersebut, seperti apakah data dapat dibaca, ditulis, atau diberi notifikasi, serta menyertakan informasi mengenai persyaratan keamanan, seperti enkripsi atau autentikasi. Sementara itu, value adalah data aktual yang disimpan dalam characteristic dan dapat diubah atau dibaca sesuai dengan properties yang ditetapkan.

2.4. Analisis Frekuensi

Analisis frekuensi merupakan metode analisis yang digunakan untuk mempelajari distribusi dari kemunculan elemen-elemen tertentu dalam suatu kumpulan data. Analisis frekuensi sering kali digunakan dengan tujuan untuk mengidentifikasi pola, tren, atau informasi tersembunyi sederhana (Inan, 2021). Inti dari Analisis Frekuensi adalah menganalisis seberapa sering simbol, kata, atau titik data tertentu muncul dan menggunakan informasi ini untuk membuat kesimpulan atau memperoleh kesimpulan. Teknik analisis ini umum digunakan dalam berbagai bidang yang berkaitan dengan data, diantaranya yaitu pada bidang kriptografi.

2.5. Analisis Entropi

Analisis frekuensi merupakan metode analisis yang digunakan untuk mempelajari distribusi dari kemunculan elemen-elemen tertentu dalam suatu kumpulan data. Analisis frekuensi sering kali digunakan dengan tujuan untuk mengidentifikasi pola, tren, atau informasi tersembunyi sederhana

(Inan, 2021). Inti dari Analisis Frekuensi adalah menganalisis seberapa sering simbol, kata, atau titik data tertentu muncul dan menggunakan informasi ini untuk membuat kesimpulan atau memperoleh kesimpulan. Teknik analisis ini umum digunakan dalam berbagai bidang yang berkaitan dengan data, diantaranya yaitu pada bidang kriptografi.

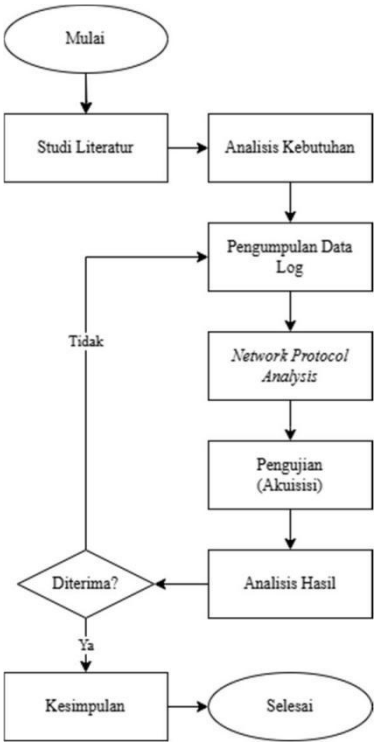
Dalam teori informasi, entropi adalah konsep kunci yang diperkenalkan oleh Claude Shannon pada tahun 1948 untuk mengukur ketidakpastian atau ketidakpastian sumber informasi (Zolfaghari et al, 2022). Shannon mendefinisikan entropi sebagai ukuran kuantitatif dari jumlah rata-rata informasi yang dihasilkan oleh sebuah variabel acak. Semakin tinggi entropi, semakin tidak pasti atau acak sumbernya, sementara entropi yang lebih rendah menunjukkan bahwa sumber tersebut lebih dapat diprediksi dan terstruktur. Secara matematis entropi dapat dituliskan pada persamaan (1).

$$H(X) = -\Sigma_{i=1}^{n} P(x_i) \log_2 P(x_i) \quad (1)$$

Persamaan (1) merepresentasikan entropi H(X), dengan $P(x_i)$ sebagai probabilitas terjadinya kejadian x_i, i = 1, 2, ..., n, dan n sebagai jumlah kemungkinan kejadian. Semakin besar nilai entropi, semakin tinggi tingkat ketidakpastian atau keragaman distribusi probabilitas X.

3. Metodologi

Tipe penelitian yang dilakukan merupakan tipe penelitian non-implementatif analitik dan bersifat eksperimental. Tipe penelitian yang bersifat non-implementatif analitik merupakan penelitian yang menitikberatkan pada investigasi terhadap fenomena atau situasi tertentu dan menghasilkan analisis ilmiah. Alur penelitian ini dapat dilihat pada Gambar 3.



Gambar 3. Alur Penelitian

3.1. Studi Literatur

Studi literatur merupakan tahap yang dilakukan untuk mengumpulkan informasi yang dibutuhkan sebagai pendukung penelitian. Sumber yang diambil dari studi literatur didapatkan dari beberapa jurnal, buku yang berkaitan dengan penelitian mengenai akuisisi data dari perangkat BLE seperti smartband.

3.2. Analisis Kebutuhan

Setelah mendapatkan informasi yang dibutuhkan dari studi literatur, dilakukan analisis kebutuhan. Analisis kebutuhan dalam penelitian ini dilakukan untuk memahami permasalahan yang menjadi urgensi dilakukannya penelitian ini secara mendalam. Dalam tahap ini, penulis mengidentifikasi permasalahan yang perlu diselesaikan oleh penelitian ini yaitu perangkat smartband hanya dapat melakukan komunikasi dengan aplikasi bawaan pada perangkat Android. Oleh karena itu penelitian ini melakukan analisis mengenai proses komunikasi dari perangkat smartband dengan aplikasi bawaan. Hasil dari analisis dapat digunakan untuk melakukan akuisisi data dari perangkat smartband melalui protokol BLE yang dapat dilakukan dengan memanfaatkan services yang disediakan pada profil GATT menggunakan fingerprint.

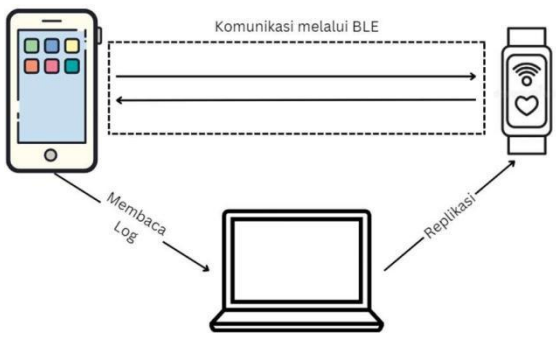
3.3. Pengumpulan Data Log

Kemudian, dilakukan pengambilan data yang akan dilakukan analisis. Data yang digunakan dalam penelitian ini merupakan data dari hasil komunikasi antara perangkat smartband Xiaomi Smart Band 8 Active dengan aplikasi bawaan yang diambil dari perangkat Android. Hasil dari data yang diambil berada dalam bentuk log yang selanjutnya akan dilakukan network protocol analysis menggunakan perangkat lunak seperti Wireshark. Data log yang diambil akan berjumlah sebanyak 10 log komunikasi antara smartband dengan aplikasi.

Perangkat keras yang digunakan dalam penelitian ini adalah smartband Xiaomi Smart Band 8 Active dengan baterai 210 mAh dan sensor Photoplethysmography (PPG), akselerometer, serta motor ERM, yang terhubung melalui Bluetooth 5.1 BLE. Logging komunikasi dilakukan pada ponsel pintar Samsung S21 berbasis Android 13, menggunakan aplikasi bawaan Mi Fitness 3.33.3. Ekstraksi log komunikasi dari perangkat Android dilakukan menggunakan Android Debug Bridge (ADB), sedangkan analisis protokol BLE tambahan dilakukan menggunakan aplikasi nRF Connect untuk memindai profil GATT pada smartband. Proses analisis lebih lanjut dilakukan pada komputer dengan sistem operasi Windows 11 menggunakan perangkat lunak Wireshark 4.4.0 untuk pembacaan log, serta bahasa pemrograman Python 3 dengan pustaka Bleak dan Asyncio untuk program akuisisi dan replikasi data.

3.4. Network Protocol Analysis

Hasil dari log yang didapatkan sebelumnya kemudian dilakukan *network protocol analysis* yang akan membahas bentuk dari data yang dikirimkan oleh perangkat Android maupun yang dikirimkan oleh perangkat smartband. Analisis ini mencakup pemeriksaan paket yang terdapat pada log, melihat *fingerprinting* yang digunakan oleh aplikasi bawaan untuk mendapatkan data dari smartband, serta jenis data yang dikirimkan maupun yang diterima oleh smartband. Data log yang telah didapatkan sebelumnya kemudian akan dilakukan pengujian replikasi yang dapat alurnya pada Gambar 4.

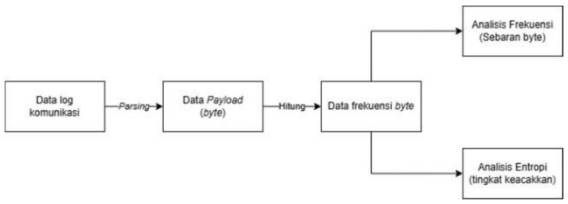


Gambar 4. Alur Replikasi

3.5. Pengujian

Gambar 4 menggambarkan pengujian alur komunikasi dan analisis data dalam sistem yang melibatkan perangkat smartband, aplikasi ponsel, dan komputer, yang terhubung melalui protokol Bluetooth Low Energy (BLE). Proses dimulai dengan komunikasi dua arah antara smartband dan aplikasi ponsel menggunakan BLE, di mana data seperti informasi detak jantung, aktivitas fisik, atau notifikasi dikirimkan antara kedua perangkat. Data komunikasi ini dicatat dalam bentuk log komunikasi pada perangkat ponsel, yang kemudian dibaca oleh komputer untuk keperluan analisis lebih lanjut, seperti memahami pola komunikasi antara perangkat. Berdasarkan analisis log tersebut, komputer juga dapat mereplikasi komunikasi yang dilakukan oleh aplikasi bawaan dengan perangkat smartband.

Dalam pengujian, sistem smartband Xiaomi Smart Band 8 Active dilakukan replication attack menggunakan data dari log yang telah diperoleh sebelumnya. Replication attack ini bertujuan untuk memantau respons sistem smartband terhadap input yang sama seperti dari aplikasi bawaan dan mengevaluasi apakah sistem memberikan respons yang serupa dengan log sebelumnya. Perlu dicatat bahwa kegagalan replikasi setelah dua frame pertama tidak secara otomatis membuktikan adanya enkripsi pada frame berikutnya, karena kegagalan tersebut juga dapat disebabkan oleh faktor lain seperti nilai sequence counter atau session identifier yang berubah pada tiap sesi komunikasi, sehingga diperlukan analisis tambahan (frekuensi dan entropi) untuk memperkuat dugaan ini.



Gambar 5. Alur Analisis

Hasil dari percobaan *replication attack* dianalisis berdasarkan respons sistem smartband terhadap input yang dikirimkan, kemudian dibandingkan dengan alur komunikasi aplikasi bawaan menggunakan data log sebelumnya. Analisis ini bertujuan untuk menentukan apakah data dari sistem smartband dapat diakses menggunakan perangkat lain selain aplikasi bawaan. Selain itu, data log dari pengiriman ulang request aplikasi bawaan ke smartband juga dianalisis untuk memahami pola sebaran data yang dikirimkan serta mengevaluasi kemungkinan adanya enkripsi data oleh sistem smartband sebelum dikirim melalui BLE. Proses analisis melibatkan metode analisis frekuensi dan entropi, seperti yang dijelaskan pada alur dalam Gambar 5.

Tahap awal analisis melibatkan parsing untuk mengekstrak payload dalam bentuk byte. Frekuensi kemunculan setiap byte dihitung untuk dua analisis utama: analisis frekuensi, yang mengkaji distribusi byte, dan analisis entropi, yang mengukur keacakan data. Analisis frekuensi menggunakan log komunikasi antara smartband dan perangkat Android, membandingkan distribusi frekuensi byte data terkirim dan diterima dengan distribusi uniform. Pola byte terenkripsi cenderung acak, sementara data tanpa enkripsi atau dengan enkripsi lemah dapat menunjukkan pola yang mudah dikenali.

Analisis entropi dilakukan untuk mengukur tingkat keacakan data log komunikasi. Data distribusi dari log dibandingkan dengan distribusi uniform. Entropi tinggi yang mendekati distribusi uniform menunjukkan data terenkripsi. Metode ini telah digunakan untuk mengukur informasi pada profil GATT (Celosia et al., 2019) dan mengidentifikasi data terenkripsi (Davies et al., 2021).

4. Hasil dan Pembahasan

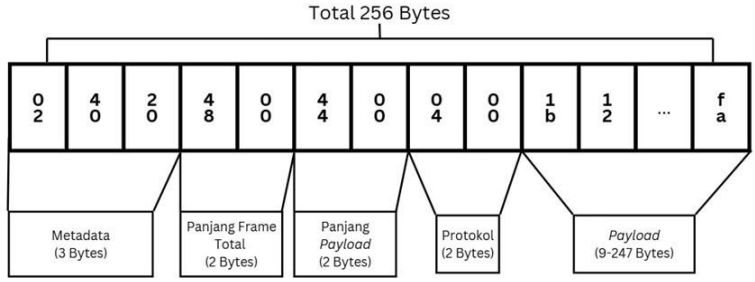
4.1. Alur Komunikasi

Komunikasi antara smartband Xiaomi Smart Band 8 Active dan aplikasi Mi Fitness dimulai dengan aplikasi mengirimkan data ke UUID 0x0052, diikuti respons dari smartband pada UUID 0x0051. Ketika alur komunikasi direplikasi pada perangkat lain seperti komputer, respons yang diberikan oleh smartband lebih terbatas dibandingkan dengan respons ke aplikasi Mi Fitness. Smartband hanya mengirimkan dua respons tambahan selain data 0x00000300, yang tampaknya diperlukan untuk melanjutkan transaksi dan akan dihentikan jika data yang diterima tidak sesuai. Berbeda dengan Xiaomi Mi Band 2 yang menyediakan data sensor seperti HRV dan akselerometer, Xiaomi Smart Band 8 Active tidak menyediakan services serupa, dan fungsi maupun nama setiap services GATT yang digunakan belum dapat diidentifikasi sepenuhnya. Untuk alur komunikasi dapat dilihat pada Gambar 6.

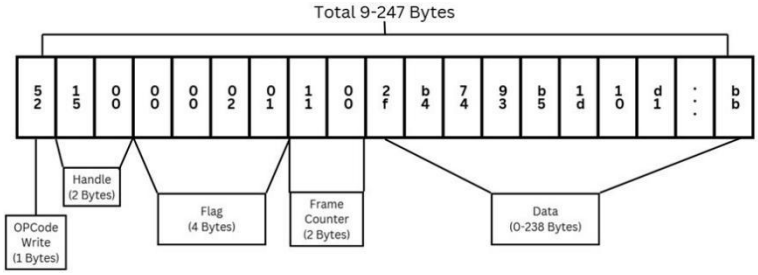


Gambar 6. Komunikasi aplikasi Mi Fitness dengan smartband.

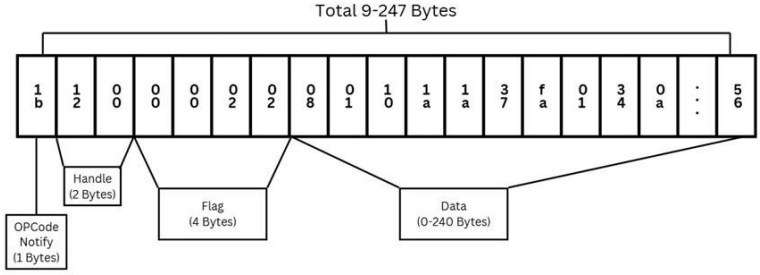
4.2. Frame & Payload BLE



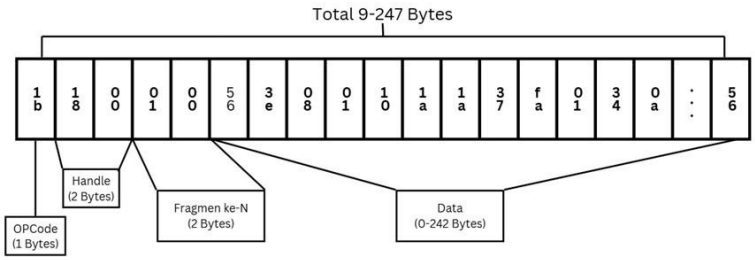
Gambar 7. Struktur umum frame BLE.



Gambar 8. Struktur payload data request.



Gambar 9. Struktur payload data response.



Gambar 10. Struktur payload data fragmen.

Gambar 7 menunjukkan struktur byte pada frame yang dikirimkan oleh smartband maupun aplikasi Mi Fitness. Bagian yang membawa data sinkronisasi berada pada payload frame. Pada payload request terdapat counter yang menghitung urutan frame yang dikirimkan aplikasi Mi Fitness, sedangkan pada payload response tidak terdapat counter tersebut. Selain itu, terdapat skema payload data fragmen yang digunakan ketika data yang dikirimkan tidak dapat dimuat dalam satu frame Bluetooth. Flag pada payload digunakan sebagai penanda jenis frame. Jenis flag pada frame BLE ditunjukkan pada Tabel 1.

Tabel 1. Jenis flag pada frame BLE

No.	Flag	Arti
1	0x00000300	Data diterima
2	0x00000202	Mengirim data
3	0x00000201	Mengirim data
4	0x00000101	Data fragment ke-n telah diterima
5	0x00000100	Data fragment telah diterima seluruhnya

4.3. Analisis Frekuensi

Tujuan analisis frekuensi byte pada request dan response adalah melihat uniformitas distribusi byte selama komunikasi. Distribusi byte dapat digunakan sebagai salah satu indikator awal untuk membedakan data plaintext dan ciphertext. Pengujian dilakukan menggunakan Chi-Squared Goodness-of-Fit Test dengan hipotesis nol (H_0) bahwa distribusi byte bersifat uniform. Statistik uji dihitung menggunakan persamaan berikut.

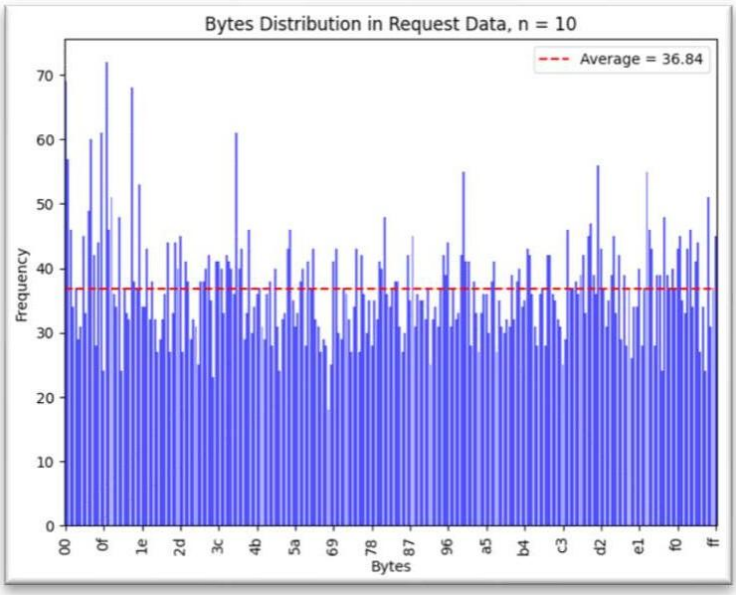
$$\chi^2 = \Sigma_{i=1}^{256} (O_i - E_i)^2 / E_i \quad (2)$$

Dengan *Degree of Freedom (DoF)* sebesar 255 dan $\alpha = 0{,}05$, hasil pengujian dirangkum pada Tabel 2, sementara distribusi frekuensi byte pada *request* dan *response* disajikan pada Gambar 11 dan Gambar 12.

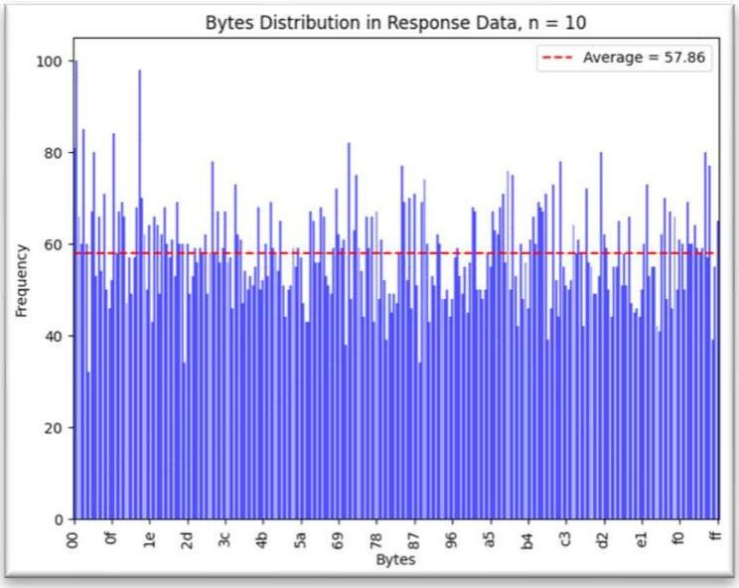
Tabel 2. Hasil Chi-Squared Goodness-of-Fit Test pada data log

Jenis data	N	χ^2 critical	χ^2 (Hasil Hitung)	p-value	Effect Size Cohen's $w = \sqrt{(\chi^2/N}$
Request	9431	293.25	435.08	1.47×10^{-11}	0,215
Response	14812	293.25	489.82	5.38×10^{-17}	0,182

Hasil kalkulasi Chi-Squared menunjukkan bahwa nilai χ^2 pada kedua jenis data (435,08 untuk request dan 489,82 untuk response) melebihi nilai χ^2 kritis (293,25), dan nilai p-value jauh lebih kecil daripada α sehingga H_0 ditolak. Dengan demikian, distribusi byte pada data request dan response tidak mengikuti distribusi uniform. Untuk menilai besarnya penyimpangan tersebut, dihitung effect size Cohen's $w = \sqrt{(\chi^2/N)}$, diperoleh w sebesar 0,215 pada data request dan 0,182 pada data response. Mengacu pada interpretasi Cohen (1988), kedua nilai ini tergolong kecil hingga sedang, sehingga meskipun penyimpangan dari distribusi uniform signifikan secara statistik, besarnya penyimpangan tergolong moderat — konsisten dengan hasil analisis entropi gabungan yang mendekati nilai maksimum.



Gambar 11. Distribusi frekuensi byte pada request.



Gambar 12. Distribusi frekuensi byte pada response.

Pengujian Chi-Squared pada penelitian ini dilakukan pada data agregat (gabungan seluruh log) untuk masing-masing jenis data, bukan pada tiap log secara terpisah. Hal ini disebabkan oleh keterbatasan ukuran sampel pada level log individual — rata-rata setiap log request hanya terdiri dari sekitar 940 byte, sehingga frekuensi harapan per kategori byte berada di bawah 5, yang menyebabkan hasil uji Chi-Squared pada level tersebut kurang andal secara statistik. Sebagai gantinya, karakteristik distribusi byte pada tiap log direpresentasikan melalui analisis entropi per log pada Bagian 4.4 (Tabel 3)

4.4. Analisis Entropi

Analisis entropi pada komunikasi antara smartband dan aplikasi Mi Fitness dilakukan untuk mengetahui karakteristik data yang ditransaksikan. Jika data tidak terenkripsi dan memiliki pola, nilai entropinya cenderung rendah. Sebaliknya, entropi yang tinggi dapat mengindikasikan data yang lebih

acak dan kemungkinan terenkripsi. Untuk data byte dengan 256 kemungkinan nilai, entropi maksimum dapat dihitung sebagai berikut.

$$H_{max} = -\Sigma_{i=1}^{256} (1/256) \log_2(1/256) \quad (3)$$

$$H_{max} = -\Sigma_{i=1}^{256} (1/256) (-8) = 8 \quad (4)$$

$$H_{max} = 8 \quad (5)$$

Nilai entropi maksimum data log adalah 8. Nilai entropi setiap log ditunjukkan pada Tabel 3.

Tabel 3. Entropi per log komunikasi

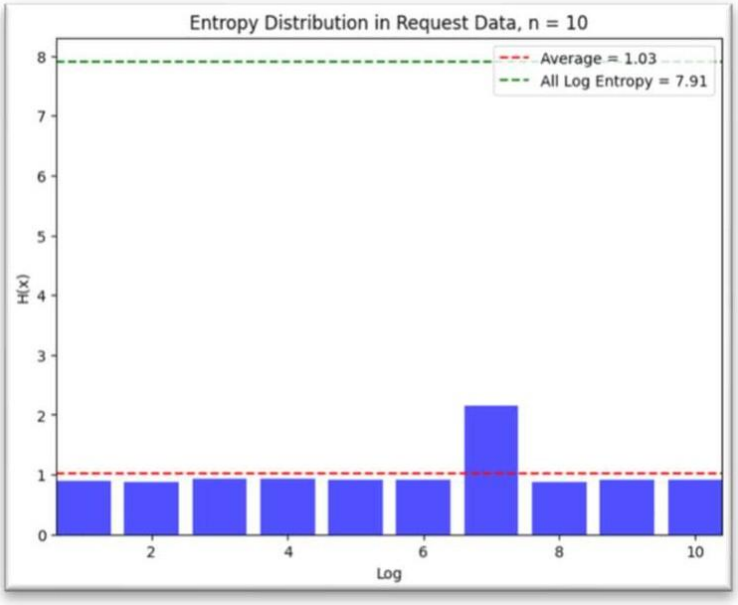
No.	Tanggal diambil	Waktu sync	Entropi Req	Entropi Rsp
1	08-11-2024	00:58:14	0.885	1.168
2	08-11-2024	01:16:51	0.877	1.433
3	18-11-2024	13:52:28	0.924	0.829
4	18-11-2024	14:05:43	0.926	0.957
5	18-11-2024	14:31:24	0.908	1.189
6	21-11-2024	00:32:38	0.905	1.102
7	21-11-2024	00:48:59	2.153	1.086
8	28-11-2024	03:21:02	0.880	2.338
9	28-11-2024	03:34:34	0.908	2.382
10	28-11-2024	03:44:15	0.909	2.448
Rata-rata			1.03	1.49

Entropi gabungan byte dari seluruh 10 log komunikasi ditunjukkan pada Tabel 4.

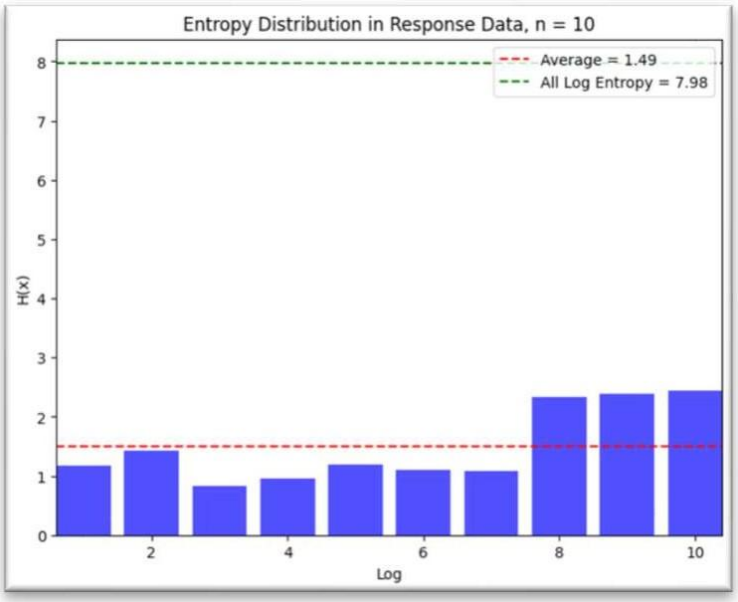
Tabel 4. Entropi total seluruh log

No.	Jenis data	Entropi
1	Request	7.910109221386434
2	Response	7.976543166151638

Visualisasi data pada Tabel 3 dan Tabel 4 ditunjukkan pada Gambar 13 dan Gambar 14.



Gambar 13. Distribusi entropi byte pada request.



Gambar 14. Distribusi entropi byte pada response.

Hasil analisis menunjukkan bahwa entropi setiap log relatif rendah, dengan rata-rata 1,03 pada data request dan 1,49 pada data response dibandingkan nilai maksimum 8,00. Hal ini menunjukkan bahwa setiap log memiliki tingkat keacakan yang rendah dan kemungkinan memiliki pola tertentu dalam pengiriman data. Namun, ketika seluruh log digabungkan, entropi meningkat menjadi 7,91 pada request dan 7,98 pada response, yang mendekati nilai maksimum. Entropi per-log rendah karena ukuran sampel byte per log relatif kecil dan variasi nilai byte terbatas akibat struktur field yang berulang, sedangkan saat 10 log digabungkan, variasi payload antarsesi meningkatkan keberagaman byte sehingga entropi gabungan mendekati nilai maksimum.

Perbedaan antara entropi log individual dan entropi gabungan menunjukkan bahwa karakteristik data berubah antarproses sinkronisasi. Entropi individual yang rendah mengindikasikan bahwa struktur byte pada tiap sesi komunikasi, seperti bagian header, flag, dan handle pada frame, bersifat tetap dan dapat diprediksi sehingga kemungkinan tidak dienkripsi. Sebaliknya, entropi gabungan yang tinggi mencerminkan variasi nilai byte pada bagian payload antarsesi sinkronisasi, yang mengindikasikan bahwa isi data aktual—seperti data kesehatan pengguna—kemungkinan mengalami proses acak atau enkripsi yang berbeda pada setiap sesi. Pola inilah yang mendasari dugaan bahwa enkripsi yang diterapkan bersifat parsial, yaitu hanya pada bagian tertentu dari frame, bukan pada keseluruhan struktur data. Berdasarkan kombinasi hasil analisis frekuensi dan entropi, data yang ditransaksikan antara smartband dan aplikasi Mi Fitness diduga berada dalam kondisi enkripsi parsial. Namun demikian, dugaan ini masih bersifat awal (preliminary) dan didasarkan pada indikator tidak langsung berupa distribusi byte yang tidak uniform serta entropi gabungan yang mendekati nilai maksimum; kesimpulan definitif memerlukan verifikasi lebih lanjut, misalnya melalui analisis statis maupun dinamis (reverse engineering) terhadap aplikasi Mi Fitness.. Bagian yang berisi data kesehatan seperti detak jantung, kalori, dan jumlah langkah diduga memiliki perlindungan lebih kuat, sedangkan informasi lain seperti indeks pengiriman dapat memiliki karakteristik yang berbeda.

5. Penutup

5.1 Kesimpulan

Penelitian ini menganalisis alur sinkronisasi Xiaomi Smart Band 8 Active karena data sinkronisasi berpotensi memuat data biologis seperti detak jantung dan jumlah langkah. Komunikasi antara smartband dan aplikasi bawaan Android berlangsung melalui dua skema, yaitu pengiriman data utuh dan data fragmen. Pada pengiriman data utuh, keseluruhan data dikirim dalam satu frame dengan flag 0x00000201 atau 0x00000202, sedangkan pada skema fragmen data dipecah ke dalam beberapa

frame. Penerima mengirimkan respons 0x00000101 ketika fragmen ke-n diterima dan 0x00000100 ketika seluruh fragmen telah lengkap. Aplikasi melakukan penulisan data ke UUID 0x0052, sedangkan smartband mengirimkan notifikasi pada UUID 0x0051 untuk skema data utuh dan UUID 0x0053 untuk skema fragmen.

Analisis frekuensi menunjukkan bahwa distribusi byte pada data request dan response tidak mengikuti distribusi uniform berdasarkan Chi-Squared Goodness-of-Fit Test. Analisis entropi menunjukkan nilai rata-rata 1,03 pada request dan 1,49 pada response, jauh di bawah entropi maksimum 8,00. Namun, entropi gabungan seluruh log mencapai 7,91 pada request dan 7,98 pada response. Perbedaan tersebut menunjukkan karakteristik yang berbeda antarlog sinkronisasi dan menjadi indikator awal atas kemungkinan adanya enkripsi parsial, meskipun kesimpulan ini masih bersifat dugaan dan belum dikonfirmasi melalui analisis langsung terhadap mekanisme keamanan pada sisi aplikasi maupun perangkat.

Penelitian berhasil memperoleh data komunikasi Xiaomi Smart Band 8 Active melalui protokol BLE menggunakan fingerprinting pada services sinkronisasi di luar aplikasi Mi Fitness. Namun, replikasi komunikasi belum mampu mengakuisisi keseluruhan data. Program fingerprinting hanya memperoleh dua frame dari sistem smartband. Hal ini diduga disebabkan oleh ketergantungan proses transformasi data berikutnya terhadap dua frame awal yang diterima dari smartband, meskipun kemungkinan penyebab lain seperti perubahan session token atau sequence counter antarsesi belum dapat dikesampingkan.

5.2 Saran

Penelitian selanjutnya disarankan menerapkan debugging pada aplikasi Mi Fitness untuk memahami algoritma yang digunakan dalam proses pembacaan data dari smartband. Selain itu, jenis smartband lain dapat digunakan sebagai pembanding terhadap struktur profil GATT dan alur komunikasi antara perangkat smartband dengan aplikasi bawaannya.

Selain itu, penelitian lanjutan disarankan melakukan verifikasi langsung terhadap dugaan enkripsi parsial ini, misalnya melalui analisis statis pada berkas APK aplikasi Mi Fitness atau pengujian dengan mengubah salah satu parameter frame awal (seperti sequence counter) untuk mengamati apakah frame berikutnya tetap dapat direplikasi, guna membedakan efek enkripsi dari efek mekanisme state lain.

6. Referensi

[1] W. R. Thompson, “Worldwide Survey of Fitness Trends for 2022,” ACSM’s Health & Fitness Journal, vol. 26, no. 1, pp. 11–20, 2022, doi: 10.1249/fit.0000000000000732.

[2] S. Huhn et al., “The Impact of Wearable Technologies in Health Research: Scoping Review,” JMIR mHealth and uHealth, vol. 10, no. 1, p. e34384, 2022, doi: 10.2196/34384.

[3] K. Guk, G. Han, J. Lim, K. Jeong, T. Kang, E.-K. Lim, and J. Jung, “Evolution of Wearable Devices with Real-Time Disease Monitoring for Personalized Healthcare,” Nanomaterials, vol. 9, no. 6, p. 813, 2019, doi: 10.3390/nano9060813.

[4] R. R. M. Putri, C.-C. Chang, H. Putra, S. Pamungkas, and D. Liang, “SmartDetect: Safe Driving by Detecting Steering Wheel Handling with a Single Smartwatch,” IEEE Sensors Journal, vol. 24, no. 10, 2024, doi: 10.1109/JSEN.2024.3379486.

[5] S. Mekruksavanich and A. Jitpattanakul, “Smartwatch-based Human Activity Recognition Using Hybrid LSTM Network,” in Proc. 2020 IEEE Sensors, 2020, doi: 10.1109/SENSORS47125.2020.9278630.

[6] G. Celosia and M. Cunche, “Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile,” in Proc. 2nd ACM Int. Workshop on Security and Privacy for the Internet-of-Things (IoT S&P’19), pp. 24–31, 2019, doi: 10.1145/3338507.3358617.

[7] C. Liu, Y. Zhang, and H. Zhou, “A Comprehensive Study of Bluetooth Low Energy,” Journal of Physics: Conference Series, vol. 2093, no. 1, p. 012021, 2021, doi: 10.1088/1742-6596/2093/1/012021.

[8] B. Pradhan, S. Bhattacharyya, and K. Pal, “IoT-Based Applications in Healthcare Devices,” Journal of Healthcare Engineering, vol. 2021, pp. 1–18, 2021, doi: 10.1155/2021/6632599.

[9] M. A. Akkaş, R. Sokullu, and H. Ertürk Çetin, "Healthcare and Patient Monitoring Using IoT," Internet of Things, vol. 11, p. 100173, 2020, doi: 10.1016/j.iot.2020.100173.
[10] A. G. Silva-Trujillo, M. Jacobo, L. Pablo, and L. Javier, "Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack," Sensors, vol. 23, no. 12, p. 5438, 2023, doi: 10.3390/s23125438.
[11] Q. Liu, Y. Zhang, and Y. Sun, "Intercepting Bluetooth Traffic from Wearable Health Devices," in Proc. 2024 IEEE Security and Privacy Workshops (SPW), pp. 267–273, 2024, doi: 10.1109/SPW63631.2024.00032.
[12] C. Zuo, H. Wen, Z. Lin, and Y. Zhang, "Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps," in Proc. 2019 ACM SIGSAC Conf. on Computer and Communications Security, pp. 1469–1483, 2019.
[13] Y. Inan, "Decoding Secret Message with Frequency Analysis," Advances in Intelligent Systems and Computing, pp. 472–479, 2021, doi: 10.1007/978-3-030-64058-3_59.
[14] B. Zolfaghari, K. Bibak, and T. Koshiba, "The Odyssey of Entropy: Cryptography," Entropy, vol. 24, no. 2, p. 266, 2022, doi: 10.3390/e24020266.
[15] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "Differential Area Analysis for Ransomware Attack Detection within Mixed File Datasets," Computers & Security, p. 102377, 2021, doi: 10.1016/j.cose.2021.102377.