Analisis Keamanan Pada Bluetooth Low Energy (Ble): Implementasi Di *Wireless Body Area Network* (WBAN) Menggunakan Watchdog Sebagai *Instrusion Detection System* (IDS)

1st Pramesta K. Kusumadani
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
pramestakharisma@student.telkomuniversity.ac.id

2nd Ida Wahidah
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
wahidah@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanfnn@telkomuniversity.ac.id

Abstrak

***Bluetooh Low Energy* (BLE) adalah protokol Bluetooth klasik dengan fitur utama konsumsi dayanya yang rendah. Namun, BLE masih rentan dalam segi keamanan. Oleh karena itu penelitian ini membuat *Intrusion Detection System* (IDS) berbasis *signature* dengan kemampuan menganalisis perilaku sistem berdasarkan peraturan di database. *Signature-Based* IDS tidak memiliki kesalahan dalam mendeteksi serangan yang telah dikenali. Penelitian ini menggunakan BLE *Mesh* dengan *Library Espressif* dan sensor DHT11 sebagai objek yang diuji. Sensor DHT11 digunakan untuk implementasi *Wireless Body Area Network* (WBAN). Topologi yang sudah dibangun akan dipantau oleh *node* watchdog, yaitu *node* IDS dengan tujuan menganalisis lalu lintas jaringan. Paket yang tertangkap oleh watchdog direkam menggunakan Wireshark kemudian IDS menganalisis lalu lintas dan memberikan peringatan. Penelitian ini menunjukan IDS mampu membaca dan mengidentifikasi lalu lintas jaringan berdasarkan log Wireshark. IDS mengindikasikan lalu lintas tersebut normal jika tidak terdeteksi paket "*Unknown*" dan "*Delta time*" di 0µs, IDS mendeteksi gangguan jika terdeteksi paket "*Unknown*" dan tidak mendeteksi "*Delta time*" di 0µs. Sedangkan IDS mendeteksi serangan jika terdeteksi paket "*Unknown*" dan "*Delta time*" di 0µs. Selain itu IDS memberikan informasi jumlah paket dan waktu penangkapan paket. Penelitian ini menghitung kualitas jaringan dan hasilnya menunjukkan jaringan ini berkualitas sangat baik.**

Kata Kunci: *Bluetooth Low Energy, Signature-Based IDS, watchdog*

Abstract

Bluetooth Low Energy (BLE) is a classic Bluetooth protocol with the main feature of low power consumption. However, BLE is still vulnerable in terms of security. Therefore, this study created a Signature-Based Intrusion Detection System (IDS) with the ability to analyze system behavior based on rules in the database. The Signature-Based IDS has no errors in detecting known attacks.This research uses BLE Mesh with Espressif library and DHT11 sensor as the object being tested. The DHT11 sensor is used for the implementation of the Wireless Body Area Network (WBAN). The topology that has been built will be monitored by the watchdog node, namely the IDS node with the aim of analyzing network traffic. The packets are captured by the watchdog who records using Wireshark then the IDS analyzes the traffic and gives warnings.This research shows that IDS is able to read and identify network traffic based on Wireshark logs. IDS finds normal traffic if "Unknown" and "Delta time" packets are not detected at 0µs, IDS detects interference if "Unknown" packets are detected and does not detect "Delta time" at 0µs. Meanwhile, the IDS detects an

attack if it detects an "Unknown" and "Delta time" packet at 0µs. In addition, IDS provides information on the number of packets and packet capture time. This study calculates the quality of the network and the results show that this network is of very good quality.

Keywords: Bluetooth Low Energy, Mesh Network, Signature-Based IDS, Watchdog

I. PENDAHULUAN

Dewasa ini perkembangan teknologi menjadi sebuah standar wajib untuk mendapati fungsi dan kualitas yang mumpuni dalam berbagai aspek kehidupan, baik dalam bidang ekonomi, Pendidikan, militer maupun kesehatan. Ditambah pandemic Covid-19 membuat seluruh aspek kehidupan bergantung kepada teknologi salah satunya di bidang kesehatan. Sehingga, diperlukannya sebuah teknologi yang tepat guna untuk mendukung kualitas kesehatan masyarakat.

Dalam satu decade kebelakang, perusahaan teknologi ikut terlibat dalam pembuatan teknologi pemantau kesehatan yaitu *smartband* dan *smartwatch.* Teknologi ini memiliki sensor untuk memantau detak jantung, kadar oksigen, suhu, dan sebagainya. Selain sensor, *smartband* dan *smartwatch* memiliki *Bluetooth Low Energy* (BLE) sebagai pengirim data sensor ke gawai. Konsep dasar ini disebut *Wireless Body Area Network* (WBAN).

BLE sendiri adalah bagian dari Bluetooth klasik yang memiliki celah kerentanan diaspek keamanannya. Pada tahun 2020, Garnelini et.al dalam judul "*SweynTooth: Unleashing Mayhem over Bluetooth Low Energy*" meluncurkan 12 kerentanan yang terjadi di BLE untuk beberapa vendor. Dua diantaranya ialah *HCI Desync Deadlock* dan *Invalid Channel Map Crash/Deadlock* yang diuji di ESP32 yang menyebabkan tidak bekerja[1]. Untuk itu perlu adanya pencegahan terkait kerentanan yang mungkin terjadi.

Signature-Based Intrusion Detection System (IDS) menjadi solusi yang dapat diimplementasikan didalam BLE guna memperingatkan jaringan jika terdeteksi serangan. Melalui peraturan yang telah dibuat untuk mendeteksi pola serangan, IDS dapat dijalankan guna mendeteksi dini serangan.

Dengan menggunakan Signature based IDS, kerentanan *HCI Desync* Deadlock dan *Invalid Channel Map* Crash/Deadlock serta ganguan lalu lintas dapat dikenali dan direkam. Sehingga dapat dilakukan pencegahan.

II. KAJIAN TEORI

a. WBAN

Wireless Body Area Network (WBAN) adalah sebuah jaringan nirkabel dengan kecepatan link 10kbps sampai 10Mbps dan mendukung 256 *node*. WBAN mampu berkomunikasi saat bergerak[2]. Berdasarkan standar IEEE 802.15.6 menjelaskan bahwa WBAN yang terdiri dari kecerdasan, teknologi sensor mikro dan nano, berdaya rendah yang dapat diletakkan atau di masukkan kedalam tubuh. WBAN biasa diaplikasikan untuk mendeteksi dini serangan jantung, asma, mengontrol diabetes dan penyakit lainnya[2]. Sehingga tenaga medis dapat memonitor, memanage, dan memberikan tindakan yang dibutuhkan ketika terjadi keadaan darurat. Pada arsitektur jaringan WBAN terdapat tiga tingkatan. Yang pertama *Intra-WBAN*. Pada level ini terdapat *Personal Server* (PS) yang bertugas untuk mentransfer sinyal sensor ketingkat kedua. PS dapat ditransmisikan sampai 2 meter dari tubuh manusia.Yang *kedua Inter-WBAN*. Tingkatan ini menjembatani antara PS dengan user via *access point* (AP). Tingkat kedua ini memungkinkan WBAN terkoneksi dengan system atau jaringan lainnya seperti internet[3] untuk model Inter-WBAN, terdapat dua macam arsitektur yaitu berbasis *infrastruktur* dan Ad-hoc. Penelitian ini menggunakan Ad-hoc sebagai arsitektur karena mampu memuat banyak *node* dan lebih flexible karena cakupan areanya cukup luas (2-100m). Yang ketiga yaitu *Beyond-WBAN Communication.* Desain komunikasi ini ideal sebagai gateway di wilayah metropolitan. Dalam ruang lingkup medis, database adalah komponen penting karena mencakup riwayat kesehatan dan profil pengguna. *Beyond-WBAN Communication* ini bergantung pada aplikasi yang dipakai. Bisa saja PS langsung berkomunikasi dengan *Beyond-WBAN Comunication* dengan menggunakan GPRS/3G/4G[3].Teknologi yang biasa digunakan di WBAN adalah jaringan nirkabel seperti Zigbee, *Wireless Local Area Network* (WLAN), *Wireless Personal Area Network* (WPAN), dan Bluetooth[2]

b. BLE *MESH*

BLE adalah *protocol* yang ada pada Bluetooth klasik dengan fitur utama konsumsi daya yang rendah. Secara kesuluruhan, Blutooth *Mesh* yang didalamnya ada BLE memiliki tiga alamat dengan fungsinya masing-masing. Yang pertama yaitu alamat *unicast*. *Unicast* dibutuhkan *node* untuk proses *provisioning*. Proses ini akan membuat *node* BLE menerima kunci jaringan untuk pertukaran pesan. Sehingga *node* BLE dapat bergabung kedalam jaringan[4]. yaitu bergabungnya *node* kedalam jaringan. Yang kedua adalah alamat grup. Alamat grup adalah *multicast address* yang mempresentasikan satu atau beberapa element[5]. Salah satu fungsinya untuk bergabung kedalam sebuah grup *node* tertentu[6]. Selama beberapa *node* saling men-*subcribe*, mereka dapat mengirim pesan menggunakan alamat *unicast* maupun alamat grup. Yang ketiga adalah alamat *virtual*. Alamat ini mencakup satu atau beberapa *node*. Biasanya digunakan untuk skenario tertentu seperti pengalamatan beberapa lampu di satu ruangan[5].

Untuk bergabung dengan jaringan, *node* perlu melakukan *provisioning* adalah proses penyediaan jaringan *Mesh* kepada *node* yang belum tersedia (*unproposioned*). Komunikasi BLE bergantung kepada dua hal. Yaitu PB-ADV dan PD-GATT[4].

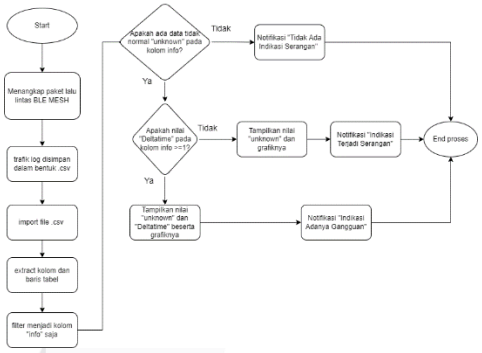
c. *Signature-Based* IDS

Intrusion Detection System (IDS) adalah sebuah software atau hardware yang digunakan untuk memantau informasi lalu lintas guna mencegah serangan dari luar. IDS dengan metode *signature-based* merupakan metode dalam mendeteksi serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam *database* atau *rule* yang sudah ada. IDS berbasis *signature* mempunyai berbagai macam signature atau pola – pola serangan yang dapat dijadikan pembanding. IDS jenis ini bekerja dengan menyadap paket yang melalui lalu lintas jaringan, kemudian membandingkan dengan pola serangan yang ada, jika paket data mempunyai pola yang sama dengan salah satu pola ang terdapat pada *rule database*, maka paket tersebut dianggap sebagai sebuah serangan. Jika tidak mempunyai kesamaan, maka paket tersebut dianggap bukan sebagai serangan[7].

III. METODE

a. Diagram Alir IDS

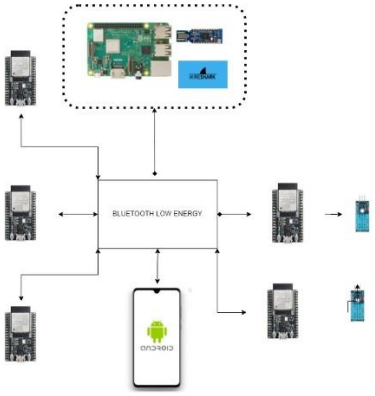
IDS yang diusulkan diimplementasikan pada Raspberry pi 3 B+ yang dihubungkan ke empat sampai lima *node* ESP32 BLE *Mesh*. Untuk menjalankan IDS dibutuhkan data lalu lintas dengan menggunakan Wireshark dan nRF5840-dongle sebagai alat bantu *sniffer*. Kemudian paket yang ditangkap diekstrak kedalam format ".csv". Dari data paket tersebut, IDS akan memfiter data paket "*unknown*" dan jumlah *delta time* yang nilainya 0µs. Jika lalu lintas memiliki paket "*unknown*" artinya terdapat masalah pada jaringan tersebut. Untuk mengetahui apakah lalu lintas terindikasi serangan atau hanya gangguan, IDS melihat jumlah *delta time* yang nilainya 0µs. Dimana, jika paket "*unknown*" memiliki *delta time* 0µs, maka diindikasikan lalu lintas telah terjadi serangan. Namun jika paket *unknown* tidak memiliki *delta time* yang nilainya 0µs, maka terindikasi lalu lintas hanya terjadi gangguan. Detail cara kerja IDS dapat dilihat pada gambar 3.1



Gambar 3.1 Diagram Alir IDS

b. Perancangan Sistem

Sistem yang diusulkan menggunakan lima *node* ESP32 dengan dua diantaranya diberikan sensor DHT11. Sedangkan untuk menyediakan Jaringan *Mesh*, menggunakan android yang telah diinstal nRF *MESH*. Raspberry Pi 3b+ digunakan sebagai *node* watchdog yaitu *node* yang memantau lalu lintas dan sebagai *node* IDS. Pemantauan lalu lintas dibantu oleh nRF52840-dongle. Untuk topologi dapat dilihat di gambar 3.2



Gambar 3.2 Topologi yang diusulkan

Skema pengujian dilakukan melalui tiga tahap dengan rincian sebagai berikut:

1. Pengujian pertama:
   Pengujian ini dilakukan menggunakan 4 ESP32 yang telah diinstal BLE *MESH* dari *Library Espressif*. Kemudian akan diambil data sebanyak 2 sesi yang mana setiap sesi dilakukan sebanyak 5 kali. Sesi pertama dilakukan selama 5 detik dan sesi kedua selama 6 detik. Tujuan dari pengujian ini agar didapat lalu lintas tanpa adanya gangguan atau serangan
2. Pengujian kedua
   Untuk mendapatkan data dari pengujian kedua, penulis menggunakan data dari Garbelini et. al, dengan Judul Penelitian *"SweynTooth: Unleashing Mayhem over Bluetooth Low Energy"*.data ini menunjukkan log serangan *HCI Desync Deadlock* dan *Invalid Channel Map Crash/Deadlock* pada ESP32.
3. Pengujian ketiga.
   Pengujian ini dilakukan menggunakan 3 *node* ESP32 yang telah diinstal BLE *Mesh* dari *Library Espressif* dan 2 *node* ESP32 dengan BLE dan sensor DHT11. Kemudian akan diambil data sebanyak 2 sesi yang mana setiap sesi dilakukan sebanyak 5 kali. Sesi pertama dilakukan selama 5 detik dan sesi kedua selama 6 detik. Tujuan dari pengujian ini untuk mendapatkan data dari lalu lintas yang terganggu. Sehingga dapat menentukan ciri-cirinya.

IV. HASIL DAN PEMBAHASAN

a. Kualitas Jaringan Pengujian Pertama

Dari tabel 4.1, didapat Rata-Rata *Throughput* pada sesi 1 tinggi diakibatkan kondisi setiap *Node* ESP32 sedang menerima perintah untuk mematikan dan menyalakan LED ketika dilakukan pengujian. Perintah ini berasal dari Proviosing yang ada pada Aplikasi BLE *Mesh* yang ada pada *Smartphone* Android. Perintah untuk mematikan dan menyalakan LED ini sangat intensif dilakukan pada saat pengujian berlangsung. Sedangkan Pada sesi 2 didapati nilai Rata-Rata *Throughput*nya kecil dikarenakan pada saat dilakukan pengujian setiap *Node* ESP32 tidak sedang menerima perintah apapun, dengan kata lain *Node* ESP32 dalam kondisi *standby* namun masih terhubung dalam Jaringan BLE *MESH*.

Perbedaan nilai Rata-Rata *Delay* yang terukur, sekitar 62.730bit/s juga terjadi akibat dari perbedaan cara pengujian yang telah disebutkan diatas. Karena perbedaan tersebut maka nilai *Delay* juga berbeda. Hal ini juga berimbas pada nilai rata-rata *Jitter* dimana walaupun nilai yang didapat sangat kecil, namun ada perbedaan sekitar 0,00127ms. Meskipun begitu bersadarkan standar Thypon, jaringan yang dibentuk masih bagus.

Tabel 4. 1 Hasil Pengujian Pertama

Parameter	**Sesi ke 1**	**Sesi ke 2**
Rata-Rata *Throughput* (Bit/s)	160169.733	97439.27248
Rata-Rata *Delay* (ms)	2.827968291	4.488513066
Rata-Rata *Jitter* (ms)	0.002995743	0.001361935

b. Kualitas Jaringan Pengujian Kedua

Berdasarkan tabel 4.2, dasil yang didapatkan pada analisis *Throughput* Serangan yang meliputi serangan *HCI Desync* dan *Invalid Channel Map* ini didapatkan Nilai *Delay* tertinggi pada serangan *Invalid Channel Map* yakni sebesar 45,8 ms sedangkan Nilai *Delay* terkecil didapatkan pada serangan *HCI Desync* yakni sebsar 31,9 ms. Jika melihat log pengujian, serangan *Invalid Channel Map* dilakukan selama 5 detik sedangkan *HCI Desync* selama 6 detik. Seharusnya nilai *HCI Desync* untuk setiap parameter QoS tinggi. Namun hasil pengujian menunjuukan hal lain. Penyebabnya adalah cara kerja serangan. *Delay* pada *Invalid Channel Map* tinggi karena terjadi *hardfault* dan kedua *peripheral* merestart. Hal ini yang menyebabkan *Delay* lebih tinggi daripada data yang lain.

Tabel 4.2 Hasil Pengujian Kedua

Parameter	***HCI Desync***	***Invalid Channel Map***

***Throughput* (Bit/s)**	13376.54907	10055.71985
***Delay* (ms)**	32.28066667	45.89473394
***Jitter* (ms)**	0.243814634	0.397836364

c. Kualitas Jaringan Pengujian Ketiga

Kondisi pengujian ketiga sama dengan kondisi pengujian pertama diaman pada sesi 1, tiga *node* BLE *MESH* menerima perintah menyalakan dan mematikan lampu. Sedangkan sesi kedua tanpa perintah. Namun hasil yang didapat cenderung nilai sesi kedua lebih tinggi daripada sesi kedua. Hal ini disebabkan karena pada sesi kesatu lalu lintas terjadi gangguan dimana saat lampu menyala, salah satu *node freeze* selama beberapa detik. Artinya ketika diberikan perintah menyalakan lampu, *node* tersebut tidak menyala, namun Ketika diberikan perintah untuk kedua kali, baru *node* tersebut menyala. Kondisi ini menyebabkan nilai *Throughput*, *Delay*, dan *Jitter* yang tidak seharusnya. Hasil dari pengujian ketiga dapat dilihat di tabel 4.3

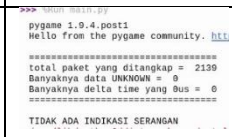
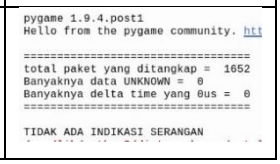
Tabel 4. 3 Hasil Pengujian Keempat

Parameter	Sesi ke 1	Sesi ke 2
Rata-Rata *Throughput* (Bit/s)	106695	155260
Rata-Rata *Delay* (ms)	2.5842	2.3495
Rata-Rata *Jitter* (ms)	0.0011	0.0006

d. Hasil Pengukuran Data Pertama Menggunakan IDS

Pengujian pada IDS untuk pengujian pertama menggunakan data pengujian pertama dengan mengambil sampel untuk setiap sesi. Dari hal tersebut didapat bahwa IDS tidak mendeteksi serangan apapun. Artinya IDS mendeteksi bahwa lalu lintas tidak terjadi serangan karena sesuai peraturan IDS, trafik tidak terdapat paket *unknown* dan tidak ada *delta time* yang nilainya 0µs.

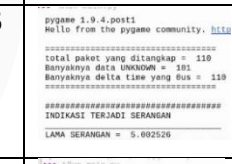
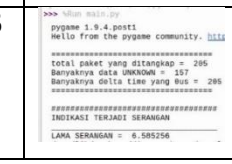
Tabel 4. 4 Notifikasi IDS pada Data Pertama

Sesi ke-	Lama Pengujian (s)	Hasil Proses Aplikasi IDS
1	5.062	
2	6.515	

e. Hasil Pengukuran Data Kedua Menggunakan IDS

Pengujian kedua menggunakan data log dari *Garbelini et. al*, dengan Judul Penelitian "*SweynTooth: Unleashing Mayhem over Bluetooth Low Energy*". Data ini menunjukkan log serangan *HCI Desync Deadlock* dan *Invalid Channel Map* pada ESP32. Dimana dari tabel 4.5, didapat bahwa IDS mendeteksi serangan dan memberikan informasi lalu lintas. IDS mendeteksi serangan dengan mengidentifikasi didalam trafik terdapat paket *unknown* dengan nilai *delta time*nya 0µs atau tidak. Artinya IDS mampu mendeteksi serangan *HCI Desync* dan *Invalid Channel Map*

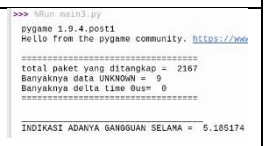
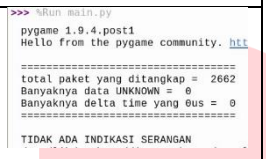
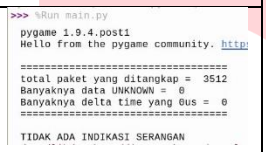
Tabel 4. 5 Notifikasi IDS paada Data Kedua

Sesi ke-	Lama Pengujian (s)	Hasil Proses Aplikasi IDS
1	5.002526	
2	6.585256	

f. Hasil Pengukuran Data Ketiga Menggunakan IDS

Pengujian ketiga menggunakan data pengujian ketiga dengan mengambil beberapa sampel setiap sesi. Dari tabel 4.6, didapat bahwa IDS mendeteksi adanya gangguan berdasarkan ada tidaknya paket *unknown* dengan nilai *delta time* tidak sama dengan 0µs. Namun dari data tersebut IDS memberikan pemberitahuan bahwa pada sesi kedua, tidak ada indikasi serangan. Hal ini terjadi karena pengujian, *node* tidak mengalami gangguan.

Tabel 4.6 Notifikasi IDS pada Data Ketiga

Sesi ke-	Lama Pengujian (s)	Hasil Akhir IDS
1	5.181008	
2	5.185174	
3	6.580891	
4	6.549808	

V. KESIMPULAN

Dari keseluruhan pengujian dapat disimpulkan bahwa IDS mampu membaca log wireshark serta mengidentifikasi ketidaknormalan paket. Aplikasi IDS yang dibangun menggunakan signature mengidentidikasi lalu lintas tidak normal didasari dari adanya peket yang "*Unknown*" dan jumlah *delta time* Ketika bernilai 0µs. IDS juga mampu memberikan notifikasi dan informasi paket. Diharapkan kedepannya IDS yang dibangun tidak lagi dilakukan secara manual untuk proses memasukkan log trafik sehingga dapat dilakukan secara real time.

REFERENSI

[1] M. E. Garbelini, S. Chattopadhyay, and C. Wang, "SweynTooth : Unleashing Mayhem over Bluetooth Low Energy LL Encryption procedure Link Layer encrypted Keys distribution procedure," 2020.

[2] P. Barsocchi and F. Potortì, "Wireless Body Area Networks," *Wearable Sensors Fundam. Implement. Appl.*, vol. 16, no. 3, pp. 493–516, 2014, doi: 10.1016/B978-0-12-418662-0.00012-X.

[3] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 113–122, 2017, doi: 10.1016/j.eij.2016.11.001.

[4] D. Hortelano, T. Olivares, and M. C. Ruiz, "Providing interoperability in Bluetooth mesh with an improved provisioning protocol," *Wirel. Networks*, vol. 27, no. 2, pp. 1011–1033, 2021, doi: 10.1007/s11276-020-02498-7.

[5] M. Wolley, "Bluetooth mesh networking," *Ericsson*, no. July, pp. 1–13, 2017.

[6] M. Baert, J. Rossey, A. Shahid, and J. Hoebeke, "The bluetooth mesh standard: An overview and experimental evaluation," *Sensors (Switzerland)*, vol. 18, no. 8, 2018, doi: 10.3390/s18082409.

[7] B. Subba, S. Biswas, and S. Karmakar, "Enhancing effectiveness of intrusion detection systems: A hybrid approach," *2016 IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2016*, 2017, doi: 10.1109/ANTS.2016.7947777.