Secure Bluetooth Communication in Smart Healthcare Systems

Subjects: Computer Science, Artificial Intelligence

Contributor: Mohammed Zubair , Ali Ghubaish , Devrim Unal , Abdulla Al-Ali , Thomas Reimann , Guillaume Alinier , Mohammad Hammoudeh , Junaid Qadir

Smart health presents an ever-expanding attack surface due to the continuous adoption of a broad variety of Internet of Medical Things (IoMT) devices and applications. IoMT is a common approach to smart city solutions that deliver long-term benefits to critical infrastructures, such as smart healthcare. Many of the IoMT devices in smart cities use Bluetooth technology for short-range communication due to its flexibility, low resource consumption, and flexibility. As smart healthcare applications rely on distributed control optimization, artificial intelligence (AI) and deep learning (DL) offer effective approaches to mitigate cyber-attacks.

smart city networks wireless communications Bluetooth artificial intelligence

1. Introduction

Cities are being transformed into *smart cities* via Internet-of-Things (IoT) technology. Smart cities use technologies for sensing, networking, and computation to enhance the quality of life and well-being of inhabitants. Such smart cities also require new service-centric computing paradigms for next-generation networks (5G, 6G, and beyond) [1]. While there are numerous networking technologies available for long-range communications, the most widely used technology for close-proximity communications is Bluetooth. Bluetooth is well suited for operations on resource-constrained mobile devices due to its low power consumption, low cost, and support for multimedia, such as data and audio streaming. Bluetooth is also widely used in smart healthcare systems to enable untethered wireless communications between smart healthcare devices. Recently, Bluetooth was prominent in its adoption for contact-tracing applications in the fight against the COVID-19 global pandemic [2].

By the year 2030 [3], the number of IoT devices is expected to surge by 124 billion. Moreover, the healthcare economy statistics predict that the market for IoT devices will grow from USD 20 billion in 2015 to USD 70 billion in 2025. It was also reported that 30.3% of the IoT devices in use are in the health sector [4]. The massive deployment of IoT devices in heterogeneous networks with multiple technologies and protocols (such as Wi-Fi, long-term evolution (LTE), Bluetooth, and ZigBee) makes the task of securing such networks very complex. Research from the Information Systems Audit and Control Association (ISACA) [5] on smart cities identified the security of IoT devices as important, as numerous smart city critical infrastructure (CI) concepts (e.g., intelligent transport, healthcare system, and energy distribution) rely on the robustness and security of smart technologies and IoT devices [6].

As the number of Internet of Medical Things (IoMT) devices increases, the network becomes congested, which leads to bandwidth and latency bottlenecks [7]. For instance, an IoMT device sends data to a medical professional for regular analysis. This transmission of data to the cloud can potentially cause latency and bandwidth congestion in the communication path [8], which could endanger the life of the patient. To address this challenge, the edge cloud concept has emerged for the IoMT paradigm. An edge cloud improves efficiency and provides more reliability for the smart healthcare system. The quick response time and reduced energy consumption will result in longer battery life for medical devices and reduce the usage of network bandwidth [9][10].

The exponential growth of IoT devices and the massive interconnectivity between such devices greatly opens up the potential attack surface for smart healthcare services that may be exploited by malicious actors. IoT devices are vulnerable to various medium- and high-severity attacks [11]. Various vulnerabilities allow the intruders to perform a wide range of attacks, such as denial of service (DoS), distributed DoS (DDoS), man-in-the-middle (MITM), data leakage, and spoofing. These attacks result in the unavailability of system resources and can lead to physical harm to the individuals when the patient is ambulance-bound or hospital-bound. According to a report from the Global Connected Industries Cybersecurity, 82% of healthcare facilities experience cyber-attacks, amongst which, 30% target IoT devices [11]. The potential weakness in the network, IoT device, and protocol allows the attackers to access the network completely in an unauthorized way (e.g., Mirai attack) [12]. Apart from these cyber-attacks, insecure operating systems, and application vulnerabilities are other major threats to the healthcare system. Investigations show that 83% of IoT devices run on outdated operating systems, and around 51% of the cyber threats in the health sector concern imaging devices, which lead to the disruption of communication between patients and medical professionals. Moreover, 98% of IoT device traffic is in plain text that can be intercepted by adversaries.

Traditional security mechanisms cannot be enforced in the IoT network because the network protocol stack itself may have numerous vulnerabilities. Zero-day attacks are very difficult to be detected by traditional security mechanisms due to computational expenses, which do not go well with the resource-constrained nature of typical IoT devices [13]. Conventional perimeter security controls only defend against external attacks, but they fail to detect internal attacks within the network. An intelligent and faster detection mechanism is required to guarantee the security of the IoT network for countering new threats before the network is compromised.

2. Security of IoMT

IoMT devices perform diverse tasks in smart healthcare systems, such as recording electrical impulses through electrocardiograms (ECGs) or monitoring blood glucose or blood pressure. For ambulance-bound patients, IoMT devices monitor the patient's activity, save critical information about the patient's physiological signals, and trigger alerts to the medical staff inside the ambulance or a remote monitoring device through the cloud. As the complete information of the patient flows in and out through the IoMT gateway [14], securing the IoMT attack surface assumes critical importance. An attacker may target the IoMT gateway to manipulate information before sending it to the doctor or to launch denial of service attacks to make the information unavailable. Such malevolent activities can put the patient's life at risk. Rasool et al. [15] reviewed various security issues of IoMT devices. The authors

describe the vulnerabilities that exist in these devices, which can be exploited by attackers easily. Herein, internal and external threats that are targeted against IoMT infrastructure are considered. Since these devices are severely resource-constrained, it is easy to render these devices unavailable by draining their battery with devastating implications [16]. Thus, the focus herein is on attacks that may drain the batteries of these devices or that make the devices unavailable due to multiple ping requests.

3. Communication in Smart Healthcare System

The typical architecture of a smart healthcare system is shown in **Figure 1**. A typical smart healthcare system comprises three domains: IoT domain, cloud domain, and user domain, which generate data, store data, and make diagnoses, respectively. The *IoT domain* consists of wireless medical devices, actuators, sensors, gateways, and other devices. Here, the focus is on acquiring patients' data from IoMT devices and transmitting it to the cloud for storage and subsequent access. The *cloud domain* is stratified by the edge and core cloud. The edge cloud is placed on the premises of the medical facility to ensure continuous connectivity and low latency, in addition to quicker diagnosis of acute cases. The core cloud provides massive storage and comprehensive analysis of data, and it helps in the diagnosis of current symptoms based on previous related records.

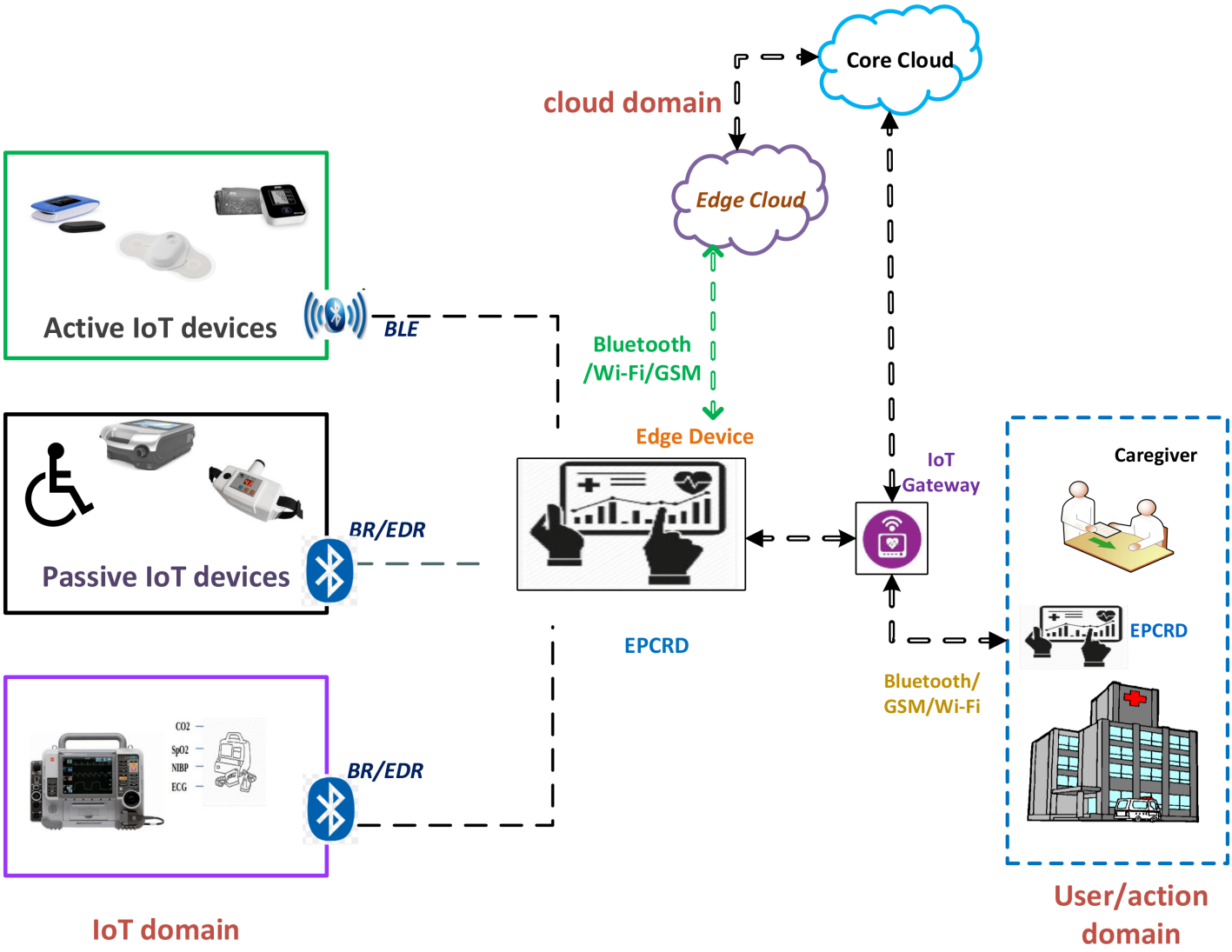

Figure 1. The use of Bluetooth and related protocols (BLE: Bluetooth low energy; BR/EDR: Bluetooth basic rate/enhanced data rate) in a typical smart healthcare system for communication between electronic patient care record device (EPCRD) and other entities over the edge and the cloud.

During IoMT communication, the vital information of a patient is maintained by an electronic patient care record device (EPCRD), which is commonly known as a Toughpad. It has the capability of integrating different communication protocols and it acts as a gateway for Bluetooth, Wi-Fi, and long-term evolution (LTE) communication. Furthermore, the EPCRD acts as an edge device that allows and enables the technologies for computation at the edge of the healthcare network. It accomplishes the tasks of caching, processing storage, computation offloading, request distribution, and delivery of the services from the cloud end to the user end. In our proposed approach, edge was leveraged and it cloud technology and deploy the intrusion detection system(s) (IDS) on the edge nodes of the healthcare system. The *user domain* delivers the processed data from other domains to the authorized clinical staff. Integration and streaming of vast volumes of data from different sources are visualized in various forms, such as graphics, images, tabular, and other representations.

Medical devices (such as defibrillators and insulin pumps) that are continuously linked with the patient for medical treatment are referred to as *active medical device(s)* (AMD). On the other hand, medical devices (such as home monitoring devices and medical beds) whose focus is on periodic monitoring of the patient physical condition and report generation are called *passive medical device(s)* (PMD). Wireless communication technologies are adopted for communication in IoT devices such as near-field communication (NFC), RFID, Wi-Fi, Bluetooth, LTE, and LoRA. Various IoMT devices use different wireless technologies. Most of the AMD and PMD utilize Bluetooth classic, V4.X, and V5. Bluetooth technology provides a generic profile for medical IoT devices to use the 2.4 GHz frequency band, as recommended by the international telecommunication unit (ITU) [17].

Bluetooth-enabled devices have two modes of operation. In the single mode, a BLE device cannot interface with a device that is operating on BR/EDR, and vice versa. Whereas in dual-mode, both BR/EDR and BLE devices can communicate with each other. However, the major concern is about security and privacy in all Bluetooth versions. Herein, the focus is on the detection of attacks against the BR/EDR and BLE, since the medical sensor and data collection devices in the considered testbed utilize this version of Bluetooth.

4. Vulnerabilities in the Bluetooth Protocols

The major vulnerability factor in Bluetooth devices is the version that is used for communication. Herein, It was described the vulnerabilities and security flaws of Bluetooth devices for different versions [18]. Few of the known vulnerabilities have been identified by researchers, such as MITM, Bluesmack, battery drain attacks, and backdoor attacks [19]. Recently, researchers identified the “SweynTooth” vulnerability affecting implantable medical devices (e.g., insulin pumps, pacemakers, and blood glucose monitors) and hospital equipment (e.g., patient monitors and ultrasound machines) that work on BLE [20]. The Bluetooth protocol has problems due to the encryption key length and improper storage of the link keys can be potentially manipulated by the adversary [12].

5. Intrusion Detection Systems

Some prior research studies on intrusion detection system(s) (IDS) dedicated to the cyber-physical system [21] or smart environments using the Wi-Fi protocol against DoS attack [21] have adopted various AI techniques, such as ML and DL. One such approach, Ref. [22], proposed a hybrid model that is based on the principal component analysis (PCA) and information gain (IG) incorporating the support vector machine (SVM), multi-layer perceptron (MLP), and instance-based learning models to identify the intrusions in the network. The model is trained and tested using the NSL-KDD, Kyoto 2006+, and ISCX 2012 datasets, and the optimal features are selected using an ensemble classifier. However, the performance of the model is evaluated with some publicly available datasets, which are not real-time datasets. Sawarna et al. [23] proposed an efficient IDS based on the deep neural network (DNN) using the principle component analysis–grey wolf optimization (PCA-GWO); it eliminates adversarial activities by providing faster alerts. Herein, it was conducted to address the problem of data dimensionality for publicly available huge datasets. They tested the NSL-KDD dataset on various ML and DNN models to detect anomalies, among which the best accuracy was attained by the DNN. Baburaj et al. [24] proposed a cloud-based

healthcare system using an SVM model to predict the health condition of a patient. The confidential data were accessed only by a legitimate user. This approach focused on data mining techniques using ML models, but not identify the anomalies in the system.

Likewise, a supervised approach for detecting intrusions in IoT devices in a smart home was proposed by Eanthi et al. [25]. In this approach, a lightweight standalone three-layer IDS framework is built using a decision tree (DT) classifier with promising results. Nevertheless, the evaluation of the proposed model is based on a simulation performed on the open-source Weka tool and the effectiveness of the IDS is not tested against real-time traffic and attacks.

6. IDS for Bluetooth Enabled Systems

Very few researchers have focused on the security perspective of Bluetooth technology, especially intrusion detection. Various attacks against Bluetooth devices are discussed below to emphasize the need for effective intrusion detection for Bluetooth-enabled medical IoT devices. Bluetooth technology provides a generic profile for the IoMT devices and it uses the 2.4 GHz frequency. It is identified as an attractive protocol for the healthcare system due to its robustness, lesser power consumption, low cost, suitability for short-distance communication, and support for data and audio streaming. Moreover, it helps in the IoT domain for machine-to-machine (M2M) communication [26]. Compromising the IoMT devices could lead to sensitive patient information being revealed through the interception and decoding of the data and audio/video streaming packets. An IDS detects malicious activities or policy violations that bypass the security mechanism on a network and is the process of monitoring and detecting unauthorized events intruding on the network. An intruder is one who escalates the privileges of the users to gain access to data or services or to control the entire network. Bluetooth-enabled systems require a different approach and standard IDS developed for other protocols are not effective due to the difference in traffic patterns and the highly constrained nature of Bluetooth devices [27].

Haataja et al. [28] proposed a Bluetooth intrusion detection and prevention system based on a set of rules by investigating Bluetooth security to discover malicious communication on the Bluetooth network. Krzysztoń et al. [29] proposed a detection system to identify the malicious behavior of Bluetooth traffic in a Bluetooth mesh network. Multiple watchdog nodes are used for cooperative decisions in different areas of the mesh network. Malicious activities are detected based on the received signal strength indicator (RSSI). However, this model encountered the problem of modeling the transmission range and RSSI parameters with obstacles, such as furniture and walls. This detection mechanism was not deployed to a variety of attacks and was evaluated in a simulated environment.

Similarly, Satam et al. [30] built a Bluetooth IDS (BIDS), where the normal behavior of the Bluetooth traffic was defined based on the n-gram approach, and malicious traffic was classified using traditional ML algorithms. This method attained the highest precision of about 99.6% and recall of 99.6%

against DoS attacks. Yet, the effectiveness of the IDS was not tested against different datasets and other attacks. An anomaly-based intrusion detection system was proposed by Psatam et al. [31] to detect multiple attacks on the

Bluetooth protocol using ML models by following the zero-trust principle. Nevertheless, the model was not tested using different attacks and datasets. Newaz et al. [32] focused on the detection of the BLE for multiple attacks using ML models to identify the abnormal behavior of the BLE traffic from the normal traffic pattern. The evaluation of the model was done on their own real-time traffic for an ideal dataset but was not tested on other datasets.

References

1. Khatua, P.K.; Ramachandaramurthy, V.K.; Kasinathan, P.; Yong, J.Y.; Pasupuleti, J.; Rajagopalan, A. Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. Sustain. Cities Soc. 2020, 53, 101957.
2. Das, D.; Zhang, J.J. Pandemic in a smart city: Singapore's COVID-19 management through technology & society. Urban Geogr. 2021, 42, 408–416.
3. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310.
4. The Ultimate List of Healthcare IT Statistics for 2020. Available online: https://arkenea.com/healthcare-statistics (accessed on 16 October 2020).
5. Smart Cities Pose New Security Challenges and Opportunities Worldwide. 2018. Available online: https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2018/global-release-smart-cities-pose-new-security-challenges-and-opportunities (accessed on 14 June 2021).
6. Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garcés, I. A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access 2020, 8, 228922–228941.
7. Limaye, A.; Adegbija, T. A workload characterization for the internet of medical things (IoMT). In Proceedings of the 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, Germany, 3–5 July 2017; pp. 302–307.
8. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile Edge Computing: A Survey. IEEE Internet Things J. 2017, 5, 450–465.
9. Khan, Y.; Ostfeld, A.E.; Lochner, C.M.; Pierre, A.; Arias, A.C. Monitoring of vital signs with flexible and wearable medical devices. Adv. Mater. 2016, 28, 4373–4395.
10. Dias, D.; Paulo Silva Cunha, J. Wearable health devices—Vital sign monitoring, systems and technologies. Sensors 2018, 18, 2414.
11. 83% of Medical Devices Run on Outdated Operating Systems. Available online: https://www.hipaajournal.com/83-of-medical-devices-run-on-outdated-operating-systems

(accessed on 1 October 2020).

12. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security Vulnerabilities in Bluetooth Technology as Used in IoT. J. Sens. Actuator Netw. 2018, 7, 28.
13. Gunathilake, N.A.; Al-Dubai, A.; Buchana, W.J. Recent advances and trends in lightweight cryptography for IoT security. In Proceedings of the 2020 16th International Conference on Network and Service Management (CNSM), Izmir, Turkey, 2–6 November 2020; pp. 1–5.
14. Yan, W.; Wang, Z.; Wang, H.; Wang, W.; Li, J.; Gui, X. Survey on recent smart gateways for smart home: Systems, technologies, and challenges. Trans. Emerg. Telecommun. Technol. 2022, 33, e4067.
15. Rasool, R.U.; Ahmad, H.F.; Rafique, W.; Qayyum, A.; Qadir, J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J. Netw. Comput. Appl. 2022, 201, 103332.
16. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Trans. Comput. Healthc. 2021, 2, 1–44.
17. Yuehong, Y.I.N.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. J. Ind. Inf. Integr. 2016, 1, 3–13.
18. Cope, P.; Campbell, J.; Hayajneh, T. An investigation of Bluetooth security vulnerabilities. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 9–11 January 2017; pp. 1–7.
19. Musale, V.P.; Apte, S.S. Security Risks in Bluetooth Devices. Int. J. Comput. Appl. 2012, 51, 1–6.
20. SweynTooth' Vulnerabilities in BLE Chips Affect Many Medical Devices. Available online: https://www.hipaajournal.com/sweyntooth-vulnerabilities-in-bluetooth-low-energy-chips-affect-many-medical-devices (accessed on 16 October 2020).
21. Franze, G.; Famularo, D.; Lucia, W.; Tedesco, F. A resilient control strategy for cyber-physical systems subject to denial of service attacks: A leader-follower set-theoretic approach. IEEE/CAA J. Autom. Sin. 2020, 7, 1204–1214.
22. Salo, F.; Nassif, A.B.; Essex, A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. Comput. Netw. 2019, 148, 164–175.
23. Swarna Priya, R.M.; Maddikunta, P.K.R.; Parimala, M.; Koppu, S.; Gadekallu, T.R.; Chowdhary, C.L.; Alazab, M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Comput. Commun. 2020, 160, 139–149.
24. Rani, A.; Viswasa, A.; Baburaj, E. Secure and intelligent architecture for cloud-based healthcare applications in wireless body sensor networks. Int. J. Biomed. Eng. Technol. 2019, 29, 186–199.

25. Anthi, E.; Williams, L.; Słowińska, M.; Theodorakopoulos, G.; Burnap, P. A supervised intrusion detection system for smart home IoT devices. IEEE Internet Things J. 2019, 6, 9042–9053.
26. Gazis, V. A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Commun. Surv. Tutor. 2016, 19, 482–511.
27. Tabassum, A.; Erbad, A.; Guizani, M. A survey on recent approaches in intrusion detection system in IoTs. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1190–1197.
28. Haataja, K.M.J. New efficient intrusion detection and prevention system for Bluetooth networks. In Proceedings of the 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, Innsbruck, Austria, 13–15 February 2008; pp. 1–6.
29. Krzysztoń, M.; Marks, M. Simulation of watchdog placement for cooperative anomaly detection in Bluetooth Mesh Intrusion Detection System. Simul. Model. Pract. Theory 2020, 101, 102041.
30. Satam, P.; Satam, S.; Hariri, S. Bluetooth intrusion detection system (BIDS). In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–7.
31. Satam, S.; Satam, P.; Hariri, S. Multi-level Bluetooth Intrusion Detection System. In Proceedings of the 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), Antalya, Turkey, 2–5 November 2020; pp. 1–8.
32. Newaz, A.K.M.I.; Sikder, A.K.; Babun, L.; Uluagac, A.S. Heka: A novel intrusion detection system for attacks to personal medical devices. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9.