SURVEY ON IMPROVING ENERGY EFFICIENCY AND SECURITY IN IoT WEARABLE DEVICES FOR DATA COLLECTION AND CLASSIFICATION

*Sam Prakash. G** [1], *Mythili. S** [2]

ABSTRACT

In this survey, the authors collected the Internet of Things (IoT) and Wireless Sensor Networks (WSN) oriented wearable sensor devices, energy efficiency and avoiding attacks. IoT wearable sensors are fitness trackers and smart-watches. Healthcare, activity recognition and individualized monitoring are few of the potential uses for the wearable IoT devices which continuously collect the data on motion, health and environmental interactions. Optimizing the energy efficiency and decreasing end-to-end latency in WSNs by the distributed clustering and energy cost functions in routing. Balancing the latency, energy cost and reliability, the multi- path routing improves. Wormhole attacks in Wireless Sensor Networks (WSNs) are difficult in detection due to their use of hidden channels. Despite the security measures like authentication and encryption, these attacks are combined with the others to become a significant threat.

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSN), Wearable Devices, Energy Efficiency, Avoiding Attacks

I. INTRODUCTION

The Internet of Things (IoT) has the revolutionized data collection, processing and analysis methods, particularly for wearable sensors. Because of the several built-in sensors, these wearable sensors continuously record the information about movements, health, and interactions with the environment [1]. Healthcare, activity recognition, and personalized monitoring are the few potential uses for the vast amount of data collected by the wearable sensors such as smart-watches, fitness trackers and health monitoring devices. Wearable sensors built on the Internet of Things (IoT) provide the seamless data collection by quickly transmitting the data to cloud-based platforms for further analysis via interaction with linked devices [2-4].

From healthcare, transportation, manufacturing and environmental monitoring, the Internet of Things (IoT) is a fresh approach which helps to standardize different kinds of technology across the sectors and environments. Internet-enabled mobile devices, sensors, actuators and RFID tags has the ability to interact with one another and the greater network defines this new kind of networking [6].

Several linked nodes make up the Wireless Sensor Networks (WSN). In monitoring or tracking the events or targets using the nodes, the first step is to deploy the nodes within a network range. The environmental domain makes an excellent use of these sensor nodes to detect the data via basic calculations [8]. The gathered data is sent to the sink node, which is called the Base Station (BS). Gateway nodes are responsible for establishing connections between the other nodes and sink nodes over the internet.

Monitoring apps and tracking applications are the two main categories of WSN applications. When used in monitoring applications, the sensor nodes keep a constant eye on their surroundings and report back to the sink with data at predetermined intervals or in response to events. In response to the user's query, an event is created while measuring a sensor node above the threshold value. In real-time tracking programmers, the data pertaining to the measurements is updated. Health, habitat, environmental, military and structural monitoring are some of the areas which makes the extensive use of WSN. Vehicles, people, military targets and animals are the most common targets in tracking the systems.

Department of Computer Applications[1],
Karpagam Academy of Higher Education, Coimbatore, India[1]
samprakashgnanaprakasam@gmail.com
Department of Computer Science[2]
Karpagam Academy of Higher Education, Coimbatore, India[2]
smythili78@gmail.com
* Corresponding Author

II. BACKGROUND STUDY

[1] the author had improved the health monitoring via the use of Energy Efficient Healthcare Data Management Method (EE-HDMM) and Internet of Things (IoT) that assisted the wearable sensor network. Efficient allocation of energy resources was recommended in order to manage increasing energy demands with finite resources. The combination of cloud computing with wearable sensor technology reduced the communication delays and made the network as an ideal platform for the mission-critical applications. The results showed that the system had efficiently detected, reduced and regulated the whole data from IoT network when used as a safety monitor. Compared to the conventional approaches, the suggested EE-HDMM had outperformed in terms of accuracy (97%), sensitivity (94%) and overall efficiency (96%). This information had been used to create the tailor-made system for every patient.

[4] these authors provided the revolutionary Internet of Things (IoT) approach for tailoring and long-term monitoring of the individual household activities. To detect the strange behaviors, the system had collected the data on various actions using the Deep Learning Techniques and a Wi-Fi wearable sensor. The described technique was intended to the extension of system such as a multi-person house that used the multiple wearable sensors to offer the personalized information. With a restricted training set, a CNN-based architecture (consisted of four convolutional layers, one fully connected layer and a 2.56-second sliding window constructed for the real-time elaboration) had achieved 97% accuracy in activity categorization. The intriguing element of discovery had demonstrated the easiest way in developing the several HAR systems suited for the variety of barriers that included the various age groups of individuals.

[6] Wearable IoT expanded the practical applications. This analysis summarized the top wearable andIoT research efforts. After study, more than 100 major works in this topic were divided into four primary groups by the practical utility. Techniques were also grouped by cluster. Wearable sensors had been accomplished with fully integrated IoT systems. Because of this, wearable and IoT integration had been used less. Cellular IoT transformed the wearable IoT sector that ignored the academics.

[15] Wearable IoT devices in the biomedical purposes was becoming popular. Despite their potential, wearable devices' battery capacity significantly restricted their longevity. The authors of this work created a wearable solar panel-specific optimization method to address the problem. Those authors had set the energy budget and accuracy limits and created an optimization problem to optimize the gesture recognition. The authors tested a prototype wearable device and constructed the tiny analytical models of energy usage and gesture detection accuracy to solve the problem. Finally, the analytical model showed that the decreasing gesture recognition length maximized the gesture recognition in quantity.

[26] Wearable technologies in the home health and ambulatory care had opened up the possibility of studying the human movement analysis. Wearable devices enabled the users in assessing their health. Sensor data analysis and identification improved the patient's quality of life evaluations. This improvement had been accomplished using the variety of approaches that included the examination of sensor data. Wearable sensors had secretly recorded the patient's routine behaviors. These metrics were highly objective and thorough than the clinical assessments. Sensor data helped the clinicians in better understanding of their patients' circumstances than the subjective approaches. In this study, those authors had looked at the wearable that automatically monitored the clinical assessments, sleep, exercise and quality of life. This research highlighted the usage of wearable sensors and automatically recognized the activities or sleeping habits by deep learning algorithms.

[17] the goal of this piece was to summarize the recent studies that addressed the topic of energy efficiency in the IoT sector. Health care, activity detection, smart settings and general solutions were the four cases that authors used to

classify IoT solutions that aimed in improving energy efficiency. This solution was not surprising that the majority current solutions were focused on the healthcare. The wearable were the first created sensor for the purpose of specific medical applications.

[25] this study examined the IoT applications in healthcare, potential to increase the service quality and the effects on established practices across the several health areas. The primary highlights of that study were as follows: 1) data processing and analysis; 2) a novel wearable sensor-based stress monitoring technique (SMA); 3) a comparison of ML algorithms; and 4) the incorporation of signals derived from wearable devices, the separation of signals from non-signals and peak augmentation. (5) Data collection, processing of data and signals, prediction, and evaluation of model performance make up the four stages of the proposed stress monitoring algorithm (SMA). Using grid search, the appropriate SVM hyper parameters (C and gamma) is found. The results showed that the top classification algorithms were XGBoost, decision trees and random forests.

[19] Wearable technology improved the health and well-being for all the ages, genders and ethnicities. Significantly, wearable helped to eliminate the health care barriers based on race, socioeconomic position and location by making timely care and treatment available to everyone. These authors examined the healthcare data transmission, cyber security risks and wearable device performance. The findings demonstrated that the researchers appreciated the IoT-based wearable devices including sensors, smart-watches, ECG monitors, blood pressure monitors and biosensors in healthcare. Academics and healthcare specialists had the long identified the present wearable technology's transformational potential, the consumer demand was driving the cutting-edge innovation to integrate the infrastructure with these gadgets. Industry insiders and academics were aware of the IoT's rapid growth in healthcare.

[12] The results showed that the patient monitoring node ran continuously and independently in both the bright and overcastted weather conditions using the suggested solar energy gathering technology. In the experimental case study, the device was operated in a continuous mode with sequential wake-up and sleep phases. The device had the total power consumption of 20.23 MW and monitored the heart rate, blood oxygen saturation (SpO2) and body temperature for the duration of 28 hours. When the sun is not present, battery is charged for every 1.2 days. Finally, the sensor node's physiological data was monitored using the Ubidots IoT platform.

[10] to summarize, wearable sensors had the potential in altering the outcomes of maternal and foetal health throughout the world. However, further research was required to ensure that the sensors were safe, reliable and cost- effective over the long run.

III. EXISTING METHODOLOGY

A. IOT data collection and classification

The following four tactics are used data collecting system, BeSmart:

On deciding the way to request measurements, the data-driven approach takes the data-accuracy trade-off into account. More specifically, in order to keep the data as precise, the expected frequency of measurement requests is altered (temporal adaptation). When several Internet of Things (IoT) sensors are located in the close proximity to one another, the collector modifies the sensors using the process measurement requests by using the spatial correlation of sensor measures. Spatial adaptation is the name of this method.

A time-driven technique ensures the elapsed time between measurements is shorter than the predetermined maximum delay and the maximum delay is proportional to the sampling rate. The elapsed time between the collector sending the measurement request and the arrival of the answer is taken into account. Several variables including the sensor's location on the IoT test bed, the measurement middleware used by the sensor and the network are impacting the time.

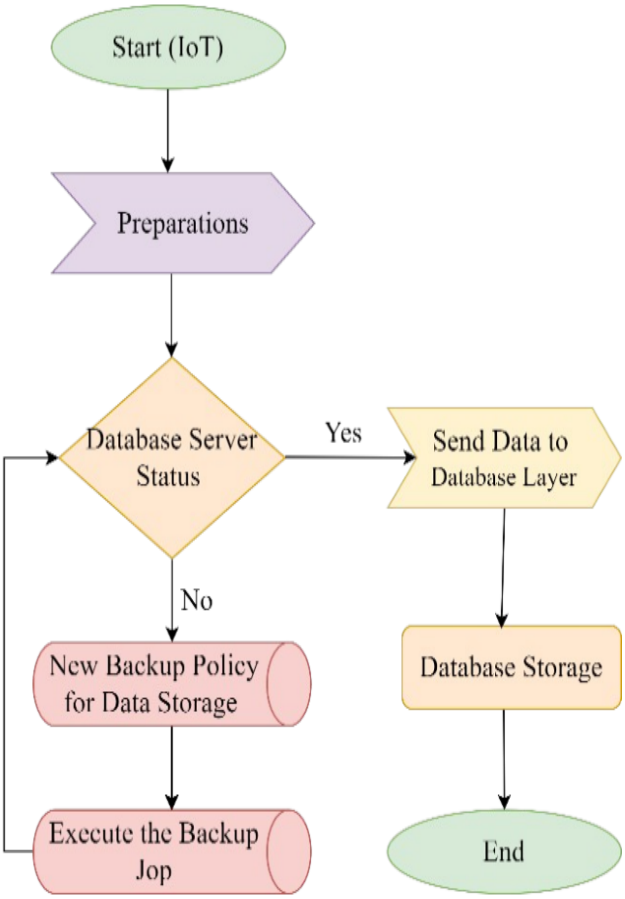

Figure 1: IoT Data collection

Privacy-driven: This approach aims to protect the users' privacy by improving the precision of their individual search results while keeping their overall statistics unchanged. To be more explicit, this approach (a) use the methods established for data-driven and time-driven strategies to reduce the frequency of data requests to a single sensor, and (b) use the differential privacy techniques to introduce the "noise" into returned findings. Information is developed for data-driven and time-driven approaches using this method.

Maximizing the net benefit—the gain for a specific data accuracy or timeliness minus the related power usage—is the purpose of the energy-driven approach. The measurement frequency affects the power consumption and the utility function is used to show the benefit for a specific data accuracy or timeliness.

A. Energy-Efficient in WSN

Improving energy efficiency is one of the primary objectives of WSN. The authors of this work provide two methods for reducing the energy use and end-to-end delays. To start, there is distributed clustering, a mechanism where the clusters choose the best cluster head according to end-to-end latency and energy usage. Adding a new energy cost function to the inter-clustering routing method solves the end- to-end latency issue. Although there are several heuristic methods for energy usage and end-to-end latency, these methods fails in providing the excellent coverage in the long term.

According to HEED (Hybrid Energy Efficient Distribution Clustering), the three primary considerations are the intersection, residual energy use and randomly selected cluster head limits. Data routing makes use of the few other methods. Efficiency of Energy Delay Optimization in the Multiple-Gateway Asynchronous Sensor Network describes both the issues. The initial step is to construct the trees which describe the optimal routing. The second one concerns the distribution of wakeup frequencies among the transmitting trees. The author provides the best way to fix the first issue. The key to solve this issue are NP-hard, polynomial-time algorithms. As a result, this brings out the second challenge.

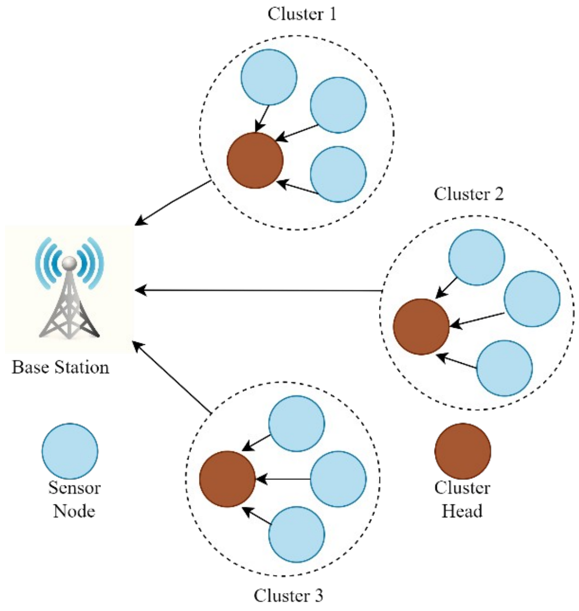

Figure 2: Energy-Efficient in WSN

Energy delay is a trade-off in WSN geographical forwarding. Choosing CH for a cluster in WSN is a multi-objective optimization issue. As soon as the sensor node respond, their data is compiled and sent to the sink. In order to dissipate the energy, l-bit receives data by the radio. Data packets of a certain length are obtained from the members using cluster heads. The advantage of cluster fuses to increase the number of members in the cluster head. The approach in this issue is delay bounded adaptive energy constrained routing. As the network is multi-path, this protocol takes the latency, energy cost and dependability into account.

Clustering techniques are used to decrease the energy consumption and end-to-end latency due to their efficacy in WSN. Clustering tree is based on the effective and energy-saving distributed scheduling method. With the help of the whole sensors' data, the author makes sure the combined packets reach the sink node as quickly as feasible. While coming to three-hop clusters, one of the many routing algorithms find the highly energy-efficient way to move from clusters to the sink.

B. Avoiding Attack in WSN

A wormhole is a particularly dangerous threat to WSN routing. In Figure 3, two or more malicious nodes working together in create a lower-latency shortcut connection is shown. This allow the nodes to pass the packets to each other and replay locally. The enemy nodes trick the neighboring nodes into the thought of the two furthest ends in the tunnel are really near to one another. If an attacker is near to the base station, they use wormholes to trick the nodes which are far from the station, into the thought in which they are only a short hop or two away, thereby disrupting the routing.These Attacks resemble the sinkholes due to the enemy promoting better paths to base station across the tunnel are common. Combinations of wormhole and sinkhole attacks are very challenging to counter. Since wormholes communicate over the unobservable private out-of-band channel, these holes are difficult for WSNs to detect. Malicious nodes encapsulate the data and use supplementary hardware such as physical connection or directional antenna in transmitting the data to one another. Wormhole attacks combine the eavesdropping and selective forwarding as both are becoming widespread. When the routing algorithms use disclosed information, the minimum hop count in the base station generates the routes and wormhole attacks in WSNs are notoriously hard to detect.

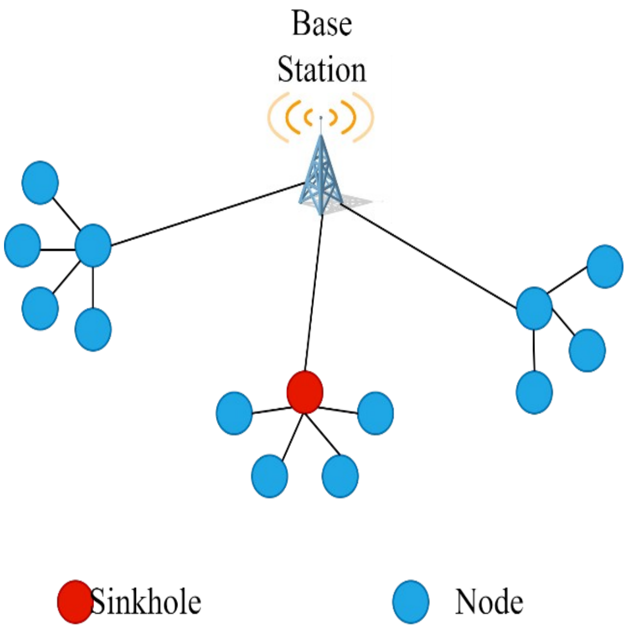

Figure 3: Avoiding Attack in WSN

Both hidden-mode and participation-mode wormhole attacks are possible. Despite authentication and encryption of the routing messages, the hidden-mode attacks still occur which makes defense against the extremely challenging ones. The malicious nodes forward the packets without the examination or modification. The bad nodes are chosen to ignore the security features of routing protocol, making the participation mode wormhole attacks very hard to detect after the nodes are underway. Initiating such an attack is more complex due to the involvement of modification in the routing packets.

Table 1: Comparison table on IoT wearable sensors devices

Authors & Year	Focus Area	Main Contribution	Key Findings
Bianchi, V., et al. (2019)	IoT for Household Monitoring	IoT and Deep Learning for activity monitoring using wearable sensors	Achieved 97% accuracy using CNN-based architecture for activity categorization with limited training data
Qaim, W. B., et al. (2020)	IoWT Energy Efficiency	Comprehensive overview of energy efficiency in IoWT applications	Most solutions focus on healthcare, with energy-saving opportunities identified in multiple sectors
Park, J., et al. (2020)	Wearable IoT for Biomedical Purposes	Optimization method for wearable devices solar panels	Analytical model suggests reducing gesture recognition maximize energy efficiency
Dian, F. J., et al. (2020)	Wearable IoT Practical Applications	Summarized over wearable IoT applications	Cellular IoT revolutionize wearable technology, but the integration was currently underutilized
Vijayan, V., et al. (2021)	Wearable in Home Health & Movement Wearable	Studied movement analysis and health assessment using wearable Explored healthcare data	Wearable offers more objective and detailed insights into health than the traditional clinical assessments Highlighted wearable tech's
Sam, M. F. M., et al. (2022)	Technology in Healthcare	transmission and wearable performance	Potential to reduce the healthcare barriers and improve the care for all the demographics
Talaat, F. M., & El-Balka, R. M. (2023)	IoT in Healthcare	Developed a new stress monitoring approach using wearable sensors	Grid search found SVM hyper parameters, with RF, DT, and XGBoost excelling in classification

IV. DISCUSSION

In this study, the four ways allows BeSmart system to properly collect the data in IoT. The data-driven approach modifies the measurement frequency to balance the accuracy by removing duplicated data from adjacent sensors via spatial adaptation. Regarding the network delays, the time-driven technique ensures the data is collected within a certain time frame. Maintaining the overall accuracy, the privacy-driven technique reduces the data searches and creates the noise in protecting the user privacy. The energy-driven technique optimizes the data accuracy and timeliness by reducing the power consumption via energy-accuracy trade-off. Wormhole attacks are particularly dangerous as they create a shortcut or "tunnel" between the two hostile nodes in a Wireless Sensor Network (WSN). These nodes work together to trick the network into the thought in which the remote nodes are nearby, disrupting the data flow routing. This is potentiallyproblematic as the allowance of attackers to selectively forward, eavesdrop and the modification of data. Wormhole attacks are difficult to detect because of their usage in private, out-of-band routes such as the physical connections or antennas. There are two types of attacks: The first one is Participation-Mode Attacks, in which the malicious node modifies the routing information, and the second one, Hidden- Mode Attacks, in which the bad node passes the packets without the modification. Hidden-Mode Attacks occur even with authenticated and encrypted message routing resulting in the complicated defense. As the Participation-Mode attacks change the routing packets, the detection is very difficult.

V. CONCLUSION

In Conclusion, this survey paper examines 26 research articles investigating the confluence of IoT data collection and classification. The BeSmart system utilizes the four key tactics for data collection: data-driven, time-driven, privacy-driven and energy-driven approaches, each optimizing the aspects like accuracy, timing, privacy and power efficiency. In Wireless Sensor Networks (WSNs), improving the energy efficiency and reducing end-to-end latency are the crucial goals. The challenges like wormhole and sinkhole attacks remain difficult in detection due to their ability of exploiting the vulnerabilities in the routing protocols. Both Hidden-Mode and Participation-Mode wormhole attacks are particularly dangerous in the requirement of advanced detection and defense strategies.

REFERENCE

[1] Ahamed, B., Sellamuthu, S., Karri, P. N., Srinivas, I. V., Zabeeulla, A. M., & Kumar, M. A. (2023). Design of an energy-efficient IOT device-assisted wearable sensor platform for healthcare data management. Measurement: Sensors, 30, 100928.

[2] Alruwaili, O., Yousef, A., & Armghan, A. (2024). Monitoring the Transmission of Data from Wearable Sensors Using Probabilistic Transfer Learning. IEEE Access.

[3] Bahalul Haque, A. K. M., Bhushan, B., Nawar, A., Talha, K. R., & Ayesha, S. J. (2022). Attacks and countermeasures in IoT based smart healthcare applications. In Recent Advances in Internet of Things and Machine Learning: Real-World Applications (pp. 67- 90). Cham: Springer International Publishing.

[4] Bianchi, V., Bassoli, M., Lombardo, G., Fornacciari, P., Mordonini, M., & De Munari, I. (2019). IoT wearable sensor and deep learning: An integrated approach for personalized human activity recognition in a smart home environment. IEEE Internet of Things Journal, 6(5), 8553-8562.

[5] Dahiya, A. S., Thireau, J., Boudaden, J., Lal, S., Gulzar, U., Zhang, Y., ... & Todri-Sanial, A. (2019). Energy autonomous wearable sensors for smart healthcare: a review. Journal of The Electrochemical Society, 167(3), 037516.

[6] Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. IEEE access, 8, 69200-69211

[7] Joy Rakesh, Y., Kavitha, R., & Julian, J. (2021). Human activity recognition using wearable sensors. In Intelligent Data Engineering and Analytics: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020), Volume 2 (pp. 527-538). Springer Singapore.

[8] Kaur, R., Shahrestani, S., & Ruan, C. (2024). Security and Privacy of Wearable Wireless Sensors in Healthcare: A Systematic Review. Computer Networks and Communications, 24-48.

[9] Khalaf, O. I., & Abdulsahib, G. M. (2020). Energy efficient routing and reliable data transmission protocol in WSN. Int. J. Advance Soft Compu. Appl, 12(3), 45-53.

[10] Liu, L., Pu, Y., Fan, J., Yan, Y., Liu, W., Luo, K., & Huang, H. (2024). Wearable Sensors, Data Processing, and Artificial Intelligence in Pregnancy Monitoring: A Review. Sensors, 24(19), 6426.

[11] Liu, Y., Wu, Q., Zhao, T., Tie, Y., Bai, F., & Jin, M. (2019). An improved energy-efficient routing protocol for wireless sensor networks. Sensors, 19(20), 4579.

[12] Mohsen, S., Zekry, A., Youssef, K., & Abouelatta, M. (2021). On architecture of self-sustainable wearable sensor node for iot healthcare applications. Wireless Personal Communications, 119(1), 657-671.

[13] Mukhopadhyay, S. C., Suryadevara, N. K., & Nag, A. (2021). Wearable sensors and systems in the IoT. Sensors, 21(23), 7880.

[14] Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2012). Energy-efficient routing protocols in wirelesssensor networks: A survey. IEEE Communications surveys & tutorials, 15(2), 551-591.

[15] Park, J., Bhat, G., Nk, A., Geyik, C. S., Ogras, U. Y., & Lee, H. G. (2020). Energy per operation optimization for energy-harvesting wearable IoT devices. Sensors, 20(3), 764.

[16] Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. Procedia Computer Science, 79, 715-721.

[17] Qaim, W. B., Ometov, A., Molinaro, A., Lener, I., Campolo, C., Lohan, E. S., & Nurmi, J. (2020). Towards energy efficiency in the internet of wearable things: A systematic review. IEEE Access, 8, 175412-175435.

[18] Rong, G., Zheng, Y., & Sawan, M. (2021). Energy solutions for wearable sensors: A review. Sensors, 21(11), 3806.

[19] Sam, M. F. M., Ismail, A. F. M. F., Bakar, K. A., Ahamat, A., & Qureshi, M. I. (2022). The effectiveness of IoT based wearable devices and potential cybersecurity risks: A systematic literature review from the last decade. International journal of online and biomedical engineering, 18(9), 56-73.

[20] Sharif, L., & Ahmed, M. (2010). The wormhole routing attack in wireless sensor networks (WSN). Journal of Information Processing Systems, 6(2), 177-184.

[21] Silva-Trujillo, A. G., González González, M. J., Rocha Pérez, L. P., & García Villalba, L. J. (2023). Cybersecurity analysis of wearable devices: smartwatches passive attack. Sensors, 23(12), 5438.

[22] Stavropoulos, T. G., Papastergiou, A., Mpaltadoros, L., Nikolopoulos, S., & Kompatsiaris, I. (2020). IoT wearable sensors and devices in elderly care: A literature review. Sensors, 20(10), 2826.

[23] Sun, F., Zang, W., Huang, H., Farkhatdinov, I., & Li, Y. (2020). Accelerometer-based key generation and distribution method for wearable IoT devices. IEEE Internet of Things Journal, 8(3), 1636-1650.

[24] Tahir, H., Tahir, R., & McDonald-Maier, K. (2018). On the security of consumer wearable devices in the Internet of Things. PloS one, 13(4), e0195487.

[25] Talaat, F. M., & El-Balka, R. M. (2023). Stress monitoring using wearable sensors: IoT techniques in medical field. Neural Computing and Applications, 35(25), 18571-18584.

[26] Vijayan, V., Connolly, J. P., Condell, J., McKelvey, N., & Gardiner, P. (2021). Review of wearable devices and data collection considerations for connected health. Sensors, 21(16), 5589.