Unraveling Sensor Correlations in Multi-Sensor Wearable Devices for Smart Anomaly Detection

Rozhin Yasaei*, Amir Hosein Afandizadeh Zargari, Mohammad Al Faruque, Fadi Kurdahi
University of Arizona*, University of California Irvine
yasaei@arizona.edu, {aafandiz, alfaruqu, kurdahi}@uci.edu

2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS) | 979-8-3503-4953-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/DCAS61159.2024.10539883

***Abstract*—In health monitoring and activity tracking technologies, wearable or implantable sensors have become indispensable, linking various human body regions to collect vital health data. Despite their potential, ensuring the security and reliability of these devices presents significant challenges, primarily due to the complexity of real-world scenarios that these systems encounter. Current approaches often rely on anomaly detection models that process historical sensor data to identify issues. However, these models tend to falter when faced with unexpected conditions or "corner cases," lacking the ability to generalize across the diverse situations encountered in everyday use. This limitation is particularly critical in wearable devices, where unexpected incidents are of paramount importance and cannot be overlooked. Addressing this gap, our research investigates multi-sensor wearable systems to understand the context of system operations and their characteristics. We introduce a context-aware approach that leverages the unique physics of the human body to identify the intricate relationships between sensors. By extracting sensor relations and patterns, our approach aims to enhance the detection of security and reliability issues, offering an advancement over traditional methods.**

***Index Terms*—Wearable Devices, Sensor Correlation, Security, Reliability, Anomaly Detection**

I. Introduction

Technological developments delegated the widespread application of Cyber-Physical Systems (CPS) in manufacturing and fostered the Industry 4.0 paradigm. Recent advances in low-power, affordable computation, and communication have encouraged the healthcare sector to pursue the industrial sector's success and take advantage of CPS [1]. Especially with the growth in the elderly population and various chronic and acute diseases globally, the health industry is changing dramatically toward point-of-care diagnosis and real-time monitoring of long-term health conditions. Therefore, wearable devices have grabbed a lot of attention, from healthcare to biomedical monitoring systems, which enable continuous monitoring of critical biomarkers for medical diagnostics. Wearable devices significantly impact sports monitoring and healthcare in obesity, cardiovascular diseases, diabetes, asthma, and Alzheimer's due to better patient monitoring, drug management, asset monitoring, tracking, and early medical interventions.

Wearable devices are an instance of CPS, which links the physical domain, the human body, to the digital world of computation. Figure 1 demonstrates the architecture of these systems, which comprises the perception layer, communication network, and application. The perception layer directly interacts with the human body, mainly including sensors and occasionally actuators. A network is expected in multi-sensor systems where wireless data sharing is required. It is facilitated by emerging communication modules such as Bluetooth, Near Field Communication (NFC), Wi-Fi, and Body Area Networks (BAN). Although single-sensor devices are also available, many wearable devices embed multiple sensors to measure various physical parameters in different body parts, such as [2]. The sensor measurement is collected by the communication network and transferred to the application for storage, display, and assessment.

Body monitoring systems must comply with certain reliability and security requirements since the system or data failure could potentially be life-threatening. Adapting the new technologies raises security and reliability concerns deriving from the interdisciplinary nature of CPS combined with the resource constraints of low-power devices [1]. Building upon the existing gap in anomaly detection methodologies, this paper introduces an innovative approach to enhance the security and reliability of multi-sensor wearable systems. Recognizing the limitations of current models that process historical sensor data without a comprehensive understanding of the system's context, our research focuses on the unique challenges presented by wearable devices. These challenges stem from the need to accurately predict and address issues across a wide array of real-world conditions, including those rare or unexpected situations that are critical to the user's health and safety.

The core insight guiding our research is the intrinsic connection between the sensors in wearable devices and the human body they monitor. Unlike in broader applications, where sensors might capture disparate data points from various sources, wearable sensors are uniquely unified in their purpose: they all measure aspects of a single, coherent system governed by well-understood physical and physiological laws. This fundamental principle—that the behavior of sensors in wearable systems should align with the known physics of the human body—provides a critical foundation for our context-aware anomaly detection model.

Our approach capitalizes on this principle, expecting sensor behaviors to adhere to the physiological and physical dynamics of the body. anticipate issues under less common, real-world conditions. Our contribution lies in developing a context-aware

979-8-3503-4953-5/24/$31.00 ©2024 IEEE

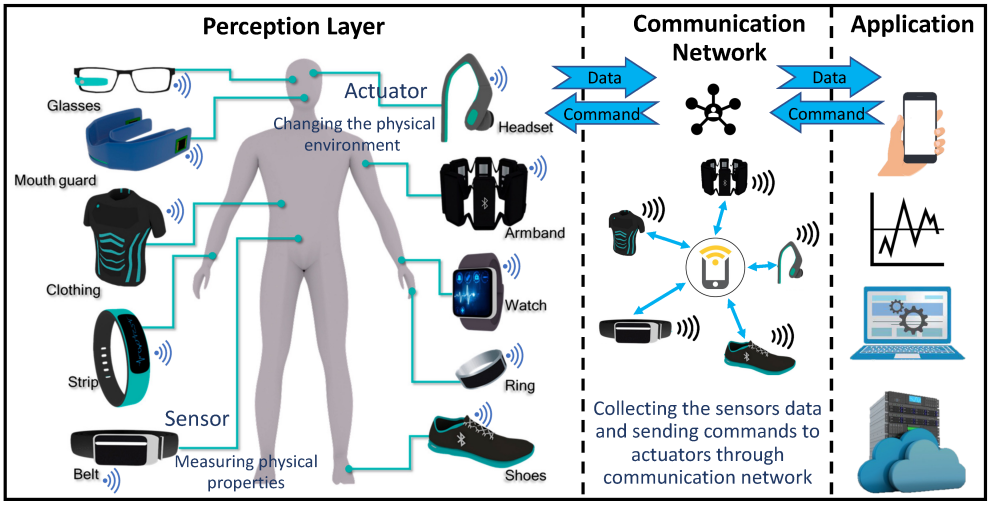


Fig. 1. The wearable devices architecture; perception layer, network, and application.

approach that, unlike its predecessors, does not rely solely on historical data. Instead, it incorporates an understanding of the wearable system's operational context and the intricate dynamics between sensors. By weaving this insight into the fabric of anomaly detection models, we enable these systems to not only recognize standard operational states but also identify and adapt to exceptional cases. Furthermore, this enriched model provides researchers with a powerful tool to delve into the origins of anomalies, facilitating a deeper understanding of the underlying causes and the nature of the issues encountered. This dual capability enhances the practical application of our approach, offering a robust foundation for both detecting anomalies and conducting subsequent investigative analysis.

II. Related Works and Background

A. Wearable Systems

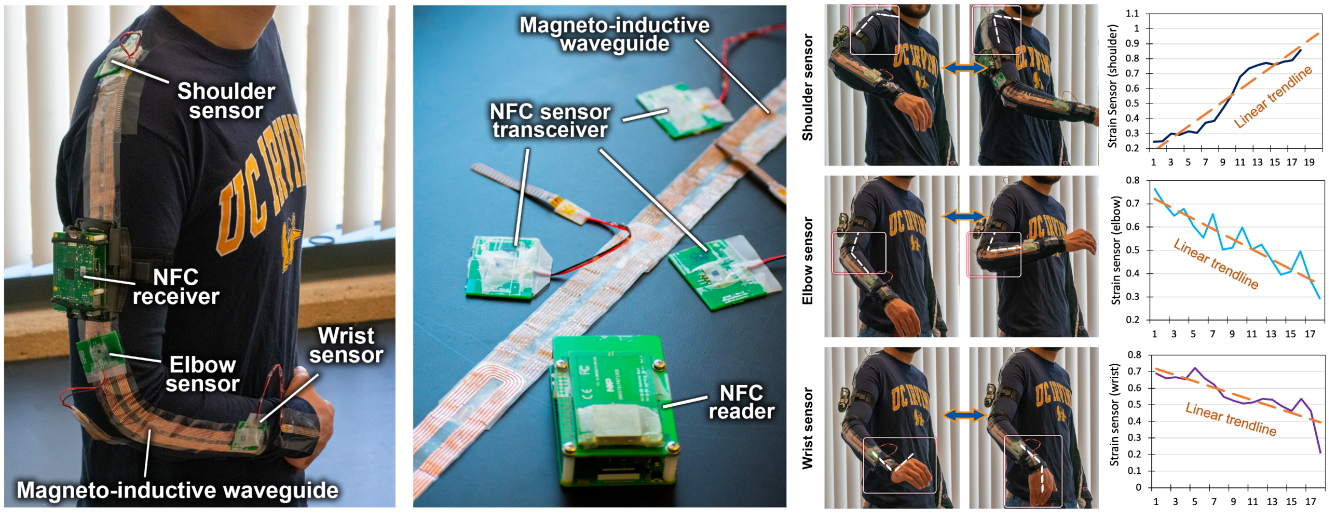
Wearable devices encompass a broad category of electronic devices designed to be worn on the body, and they are intended to provide users with convenience and ease of access. These devices are user-friendly computing devices and are considered among the most personal and intimate electronic gadgets due to their proximity to the user. The increasing adoption of wearable devices has brought concerns related to their security to the forefront. In a study conducted by Lee et al. [3], the vulnerabilities of wearable devices are examined across three primary factors: the device itself, the communication between the device and servers, and the servers hosting the wearable services. The authors' investigation led to the identification of three novel attack scenarios targeting wearable services. These scenarios were subsequently applied to real commercial smart bands used for healthcare monitoring, and the results demonstrated the effectiveness of these attacks. These attacks could compromise the wearable device and expose personal user information, including health data.

Furthermore, a comprehensive overview of security and privacy threats faced by wearable devices is presented in [4]. This study includes a security analysis of various wearable devices, such as Google Glass and Fitbit. The authors argue that due to wearable devices' limited computational power and bandwidth, their security posture is comparatively weaker than that of other computing devices. One of the primary challenges in ensuring privacy and security in wearable devices, as highlighted by the authors, is authentication, particularly given their interactions with other devices like smartphones. In wearable devices, proximity to the human body introduces a unique set of security considerations. In the work by Mills et al. [5], the authors delve into the security aspects of wearable devices, emphasizing the potential for harm to individuals. They assert that wearable devices represent a distinct category of electronic devices with a tangible risk of causing physical harm to the wearer, in addition to posing threats to data security and the devices themselves. The authors call for a more in-depth examination and development of security measures to safeguard the well-being of wearable device users.

B. Anomaly Detection

Conventionally, statistical or probabilistic methods are utilized for anomaly detection [6] in which a statistical [7], or probabilistic model [8] is mapped on the normal data. The model captures the system's normal behavior, and its comparison to the new data point reveals if the data point is statistically unlikely or has a low generation probability. Recently, the advancement in machine learning has fostered the application of deep learning to detect anomalies. Various techniques for density measurement and clustering are proposed in the literature, such as K-Nearest Neighbor (KNN) [9], Local Density Factor [10], reverse KNN [11], and deep embedding for clustering [12].

In another approach, a predictive model is trained on normal data to learn the features of the normal state by studying the recent and long-term trends of the system. Later, it evaluates the normality of data instances by their consistency with the predictive model expectation, and substantial deviation is denoted as an anomaly. The predictive models are usually constructed based on recurrent neural network [13], AutoEncoder (AE) [14], [15], and convolutional neural network [16], [17].



(a) (b) (c)

Fig. 2. Experimental setup, (a) designed wearable system, (b) detailed view of the setup, (c) movement range for different sensors

III. Our Approach

Health monitoring and activity tracking technologies heavily rely on the integration of wearable or implantable sensors that establish connections with various regions of the human body, including the potential to link multiple individuals. These interconnected sensors form multi-node networks, enabling biometric data collection from human subjects and the objects they interact with. Establishing secure and reliable communication links among these nodes, commonly referred to as BANs, is crucial for the real-time parsing of biometric information [18], [19].

In our wearable system, the specific requirements of BANs impose a unique set of constraints on the performance of the magneto-inductive waveguide. This waveguide must exhibit high flexibility, remain impervious to bodily motion, offer ease of extension, and adopt a microelectronics-free design. To address these constraints, we have designed multiturn flexible planar coils composed of metal foils (aluminum and/or copper) as resonators to seamlessly integrate into the clothing textile. The propagation of magneto-inductive waves through arrays of magnetically coupled resonators allows for more complex network architectures, accommodating the relative placement of resonators and introducing horizontal distances within the network between the reader and sensor nodes. Unlike traditional BANs that rely on wired connections between coils, our inter-resonator magnetic coupling facilitates intricate network structures with user-friendly scalability. This approach enables signal paths to span multiple layers of disconnected clothing, setting it apart from other textile-based BANs reliant on wire or conductive thread-based connections. Establishing secure and reliable communication links among nodes is crucial for the real-time parsing of biometric information [18], [19]. The robustness of a BAN is contingent upon several key attributes: user comfort, adaptability to existing clothing, adherence to established standards [20], node sampling rates, and wireless power capabilities [21].

We have employed a software-based Time Domain Multiple Access (TDMA) technique to enable seamless switching between sensing nodes. The controlled surface propagation of magneto-inductive waves eliminates the need for multiple near-field antennas connected by wires [22], [23], or complex antenna switching schemes requiring active microelectronics. This design allows conventional NFC-enabled smartphones to serve as compatible readers. The wireless efficiency of the network was evaluated through measurements of the NFC Packet Reception Ratio (PRR), defined as the ratio of successfully received packets by the reader to the total transmitted packets. Each packet encompasses sensor information from all transponders within the network during a single refresh. In practice, limitations such as strain sensor latency and hysteresis affect performance at higher frequencies. Furthermore, the TDMA approach permits the connection of up to 12 sensors along the network, with trade-offs between sampling rate, the number of sensors, and packet loss. The magneto-inductive BAN can be tailored to individual needs and produced cost-effectively, fostering personalized wearable networks.

This versatile ecosystem holds the potential to facilitate real-time healthcare and status monitoring in diverse settings, including clinical, athletic, and daily routines. For instance, integration into hospital patient uniforms could enable seamless patient monitoring through the effortless placement and rearrangement of sensors on clothing. Professional sports organizations may develop highly customized networks that are aligned with their branding and optimized to cater to specific athletic training and monitoring requirements. The vinyl-based elements empower users to create and rearrange networks without needing specialized equipment, adaptable for both local and long-range monitoring across the body. Sensing nodes can be easily interchanged or repositioned, facilitating plug-and-play measurements of various relevant parameters.

In addition to designing and implementing this wearable

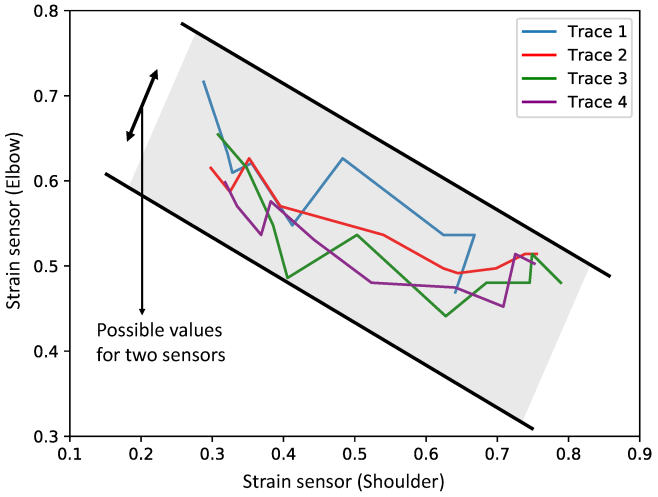


Fig. 3. Correlation between elbow and shoulder movement

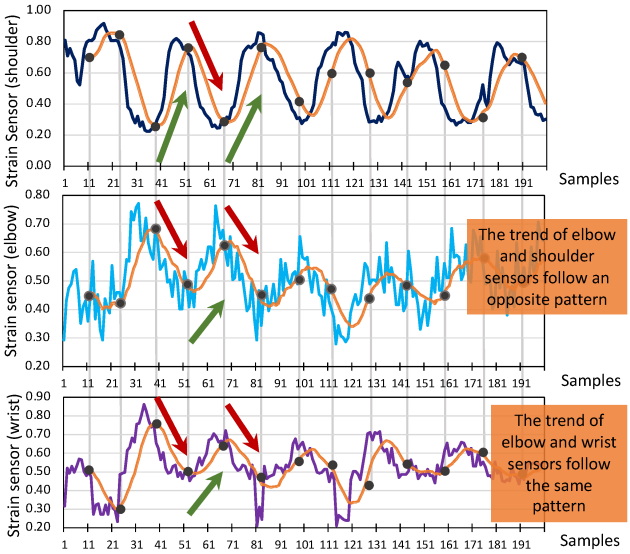


Fig. 4. Values of the Sensors placed on shoulder, elbow, and wrist.

system, We present a methodology to detect anomalies in such multi-sensor systems. This system is designed to process a sequence of sensor readings as input data. While these sensors exhibit distinct characteristics, it is important to note that the values they generate can exhibit interdependencies. For instance, changes in one sensor's reading can have ripple effects on the readings of other sensors. The proposed system capitalizes on the Context Learning model, which considers a variety of sensor readings over a specific period and leverages this information to forecast the values of these sensors at the subsequent time stamp. Notably, this model goes beyond the individual attributes of each sensor by understanding the intricate relationships among different sensors. The predicted sensor values serve as the input for an anomaly detection module. We study the system through different data analysis techniques elaborated in Section IV and devise a strategy that determines the safe zones and threat zones of sensor data.

IV. Data Analysis and Context Extraction

A. Experimental Setup and Dataset

In Section III, we discussed the experimental setup utilized to investigate human arm movements. In this context, we aim to assess the arm's motion comprehensively. We employed coils to cover the entire arm, as illustrated in Figure 2(a). Subsequently, we strategically placed strain sensors at crucial arm joints, including the elbow, shoulder, and wrist. Strategically positioned at the mentioned joints, these three sensors are well-suited to monitor a wide spectrum of arm movements. Figure 2(c) visually represents the start and end points of motion, along with the associated range of motion and sensor values for each action.

Our approach involves a custom-designed PCB equipped with an RF430frl152 NFC chip, an NFC antenna, and a strain sensor. We utilize a PN7150 NFC reader connected to a Raspberry Pi to retrieve data from these sensors. For the data collection phase, we enlisted the participation of ten individuals, each aged 25 to 41 years. These participants were instructed to perform arm movements for a duration of 10 minutes, encompassing various directions and ranges of motion. By incorporating the clothing setup and the three strategically positioned strain sensors (located at the elbow, shoulder, and wrist) as described in Section IV-A, we recorded these movements at a frequency of 8Hz.

B. Wearable System Context and Sensors Relation

We investigate the importance of context-aware anomaly detection for wearable devices in a setup explained in Section III. In this system, three strain sensors are attached to a wrist, elbow, and shoulder wearable device to monitor human body movements. An NFC network is implemented on the device to gather the measurement frequently. Figure 4 demonstrates the three sensor recordings in a time interval involving frequent movements. To analyze data further, we plot the trendline of each time-series data by calculating the moving average of data with a window size of 10. The averaging process reduces the noisy local variations and reveals the general pattern. The results indicate the hidden relationships among the sensors. The elbow and wrist sensors are directly related and follow a similar pattern of changes, while the shoulder sensor changes pursue a reverse pattern. This correlation relies on the shared context among sensors, which is common in wearable sensors. The interaction with the physical world highlights the importance of context in CPS because the same environmental factors influence multiple components. Consequently, their behavior and data would show correlations. In large-scale CPS, it is challenging to discover the shared context between sensors due to widespread sensor distribution. However, sensor correlations are evident in wearable devices because the sensors are attached in close proximity and observe a single physical system, the human body.

During each movement, several muscles and joints are engaged; as a result, these movements influence multiple

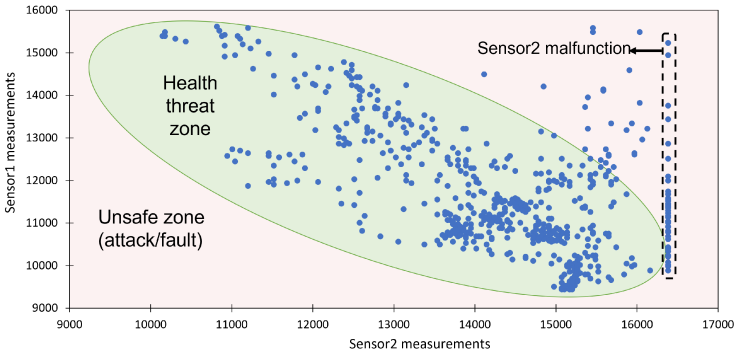


Fig. 5. Distinction of unsafe zone and health.

sensors positioned at various joints. This implies that the readings from these sensors exhibit correlations with each other. As illustrated in Figure 3, this interrelation between the values of sensors attached to the elbow and shoulder is depicted. Notably, these sensor values tend to cluster within specific ranges, reflecting the constrained set of movements that the human body is capable of. Leveraging a multi-sensor system and capitalizing on the interrelatedness of sensor values equips us with the capability to detect abnormal situations. To expound further, let's consider a scenario where one of the sensors is under attack. Given the intrinsic correlations between sensor values, detecting this attack by observing the other sensors' values is feasible. Figure 5 demonstrates the result of our data analysis in which we divide the data space into two zones, determining the state of the wearable system.

V. Conclusion

This study addresses the critical issues of reliability and security in wearable devices by implementing anomaly detection and diagnosis. Wearable devices interact with the physical world and share a contextual environment. This shared context is particularly pronounced in wearable devices since the physical environment remains consistent across all components, primarily the human body. By embedding this comprehension into our anomaly detection models, we enable the system to accurately identify both standard and exceptional states. Furthermore, this refined approach facilitates researchers in delving deeper into the anomalies, allowing them to investigate the underlying causes and precisely classify the nature of the issues encountered.

References

[1] J. I. Jimenez, H. Jahankhani, and S. Kendzierskyj, "Health care in the cyberspace: Medical cyber-physical system and digital twin challenges," in *Digital twin technologies and smart cities*. Springer, 2020.

[2] A. Hajiaghajani, A. H. Afandizadeh Zargari, M. Dautta, A. Jimenez, F. Kurdahi, and P. Tseng, "Textile-integrated metamaterials for near-field multibody area networks," *Nature Electronics*, 2021.

[3] M. Lee, K. Lee, J. Shim, S.-j. Cho, and J. Choi, "Security threat on wearable services: Empirical study using a commercial smartband," in *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, 2016.

[4] K. W. Ching and M. M. Singh, "Wearable technology devices security and privacy vulnerability analysis," *International Journal of Network Security & Its Applications*, 2016.

[5] A. J. Mills, R. T. Watson, L. Pitt, and J. Kietzmann, "Wearing safe: Physical and informational security in the age of the wearable device," *Business Horizons*, 2016.

[6] M. Markou and S. Singh, "Novelty detection: a review—part 1: statistical approaches," *Signal processing*, 2003.

[7] M. L. Han, J. Lee, A. R. Kang, S. Kang, J. K. Park, and H. K. Kim, "A statistical-based anomaly detection method for connected cars in internet of things environment," in *Internet of Vehicles - Safe and Intelligent Mobility*. Springer International Publishing, 2015.

[8] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology," in *2016 IEEE International Conference on Communications (ICC)*, 2016.

[9] S. Ramaswamy, R. Rastogi, and K. Shim, "Efficient algorithms for mining outliers from large data sets," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, 2000.

[10] L. J. Latecki, A. Lazarevic, and D. Pokrajac, "Outlier detection with kernel density functions," in *International Workshop on Machine Learning and Data Mining in Pattern Recognition*. Springer, 2007.

[11] M. Radovanović, A. Nanopoulos, and M. Ivanović, "Reverse nearest neighbors in unsupervised distance-based outlier detection," *IEEE transactions on knowledge and data engineering*, 2014.

[12] J. Xie, R. Girshick, and A. Farhadi, "Unsupervised deep embedding for clustering analysis," in *International conference on machine learning*, 2016.

[13] W. Lu, Y. Cheng, C. Xiao, S. Chang, S. Huang, B. Liang, and T. Huang, "Unsupervised sequential outlier detection with deep architectures," *IEEE transactions on image processing*, 2017.

[14] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining*, 2017.

[15] R. T. Ionescu, F. S. Khan, M.-I. Georgescu, and L. Shao, "Object-centric auto-encoders and dummy anomalies for abnormal event detection in video," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019.

[16] D. Abati, A. Porrello, S. Calderara, and R. Cucchiara, "Latent space autoregression for novelty detection," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019.

[17] W. Liu, W. Luo, D. Lian, and S. Gao, "Future frame prediction for anomaly detection–a new baseline," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018.

[18] M. R. Yuce, "Wearable sensors get connected with plasmons," *Nature Electronics*, 2019.

[19] J. Kim, A. S. Campbell, B. E.-F. de Ávila, and J. Wang, "Wearable biosensors for healthcare monitoring," *Nature biotechnology*, 2019.

[20] M. R. Yuce, "Implementation of wireless body area networks for healthcare systems," *Sensors and Actuators A: Physical*, 2010.

[21] H.-J. Kim, H. Hirayama, S. Kim, K. J. Han, R. Zhang, and J.-W. Choi, "Review of near-field wireless power and communication for biomedical applications," *IEEE Access*, 2017.

[22] K. Aslanidis and V. N. Gunasegaran, "Trf7970a nfc reader antenna multiplexing," *Texas*, 2016.

[23] J. Wyatt, "Trf7960a rfid multiplexer example system," 2012.