Towards a UHF RFID Electromagnetic Fingerprint-Based Digital Twin Resolver

Shah Md Nehal Hasnaeen
Department of Electrical and Computer Engineering
Idaho State University
Pocatello, ID, United States
shahmdnehalhasnae@isu.edu

Suman Neupane
Department of Electrical and Computer Engineering
Idaho State University
Pocatello, ID, United States
sumanneupane@isu.edu

Andrew Chrysler
Department of Electrical and Computer Engineering
Idaho State University
Idaho Falls, ID, United States
andrewchrysler@isu.edu

***Abstract*—The viability of utilizing the frequency domain electromagnetic (EM) fingerprint of passive Ultra-High Frequency (UHF) Radiofrequency Identification (RFID) tags as the basis for a digital twin resolver is explored. A framework is laid out for a digital twin resolver utilizing the XGBoost machine learning algorithm to classify EM fingerprints of tags attached to physical objects to associated digital counterparts. Preliminary analysis indicates an ability to differentiate between RFID tags based on the Electronic Product Code (EPC) with 99% overall accuracy, meaning a machine learning model can act as a resolver to identify digital twins by analyzing and classifying EM fingerprints with differing EPC content if the training database is large enough.**

Keywords—Digital Twin, RFID, Electromagnetic Fingerprint, Machine Learning.

I. INTRODUCTION

A digital twin (DT) is a replica of a physical object in the digital or virtual world. The purpose of the digital twin is to provide necessary feedback which can then be utilized to improve upon its physical twin [1]. Even though the concept of the DT was first created in 2003 by Michael Grieves at the University of Michigan [2], it has become a subject of interest among researchers and academics recently with the proliferation of IoT and machine learning (ML) [3]–[6]. Based on the sophistication of the physical system different levels of DT can be created including pre-digital twin, adaptive digital twin, and intelligent digital twin [7]. A pre-digital twin emphasizes risk mitigation while the adaptive and intelligent digital twins focus more on development via ML and reinforced learning. Digital twin technology has realms of possibilities in smart manufacturing, Industry 4.0 [8], safety management [9], automation [10], reinforced learning [11], and more. Digital twins can be created using two main categories: (1) data-driven digital twins and (2) model-based digital twins [12]. Model-based digital twins usually maintain the connection to their physical twin to represent the dynamic and static behavior of the system whereas data-driven digital twin uses data information from different sensors to model their physical twin which is seen to demonstrate both known and unknown parts of the physical system [13]. In practice, both model-based and data-driven digital twin models are used in tandem to model the overall physical system [7].

Radio Frequency Identification (RFID) tags utilize backscatter for data transmission and object identification [14]. RFID is utilized in IoT systems in the ultra-high frequency (UHF) band (860-960 MHz) [15]. Passive RFID tags are significantly popular because of their low cost, no battery requirement, memory availability in the form of Electronic Product Code (EPC) and user memory banks, and versatile applications on different fronts like localization [16], supply chain management, IoT [17], and more. Of particular importance is the EPC memory bank, which acts as memory allocated for an idiosyncratic numerical code for universal identification of products [18]. Passive RFID tags have been utilized in several DT models for applications, such as leakage detection using coarse-grained backscatter signal which is tested in real-world digital twin system Pavatar [19][20], a unified modeling language (UML) based framework for modeling digital twins [21], digital twin of paper products warehouse [22], digital twin representation model of retail and apparel industry [23]. These utilized the tracking function via EPC memory content of the RFID tags in the creation of data-driven digital twins. Reliance on such a cataloging convention alone runs the risk of tag cloning. Cloning of RFID tags remain a key problem going forward for digital twins.

A virtually non-replicable property of RFID tags suitable for cloning prevention in a DT is their electromagnetic (EM) fingerprint [24]. EM fingerprint refers to signal data obtained from excited RFID tags in the time or frequency domain. The uniqueness of these signals taken at any instance can be recognized by smart machine learning algorithms. This EM fingerprint is dependent on multiple factors such as the EPC memory banks and the manufacturing process of the tags.

This paper lays the foundations for an RFID EPC EM fingerprint-based, data-driven digital twin resolver which can be implemented to create any level of the digital twin. The resolver will be able to locate the digital object based on frequency spectrum signal strength data via passive tags

embedded or attached to the physical counterparts, making it cost-effective. Previous digital twin resolvers based on RFID focused on the use of cataloging and inventory management, limiting use cases to industrial supply chains or specific products. The proposed resolver will be able to create and allocate unique keys for all digital twins. Multiple keys cannot be made for the same digital twin as each key will be determined by the signal emitted by the attached tag, which should be only replaced if not functioning. The EM fingerprint cannot be replicated just by knowing the memory content and configuration of the embedded passive tag. Therefore, this DT model increases resistance to RFID tag cloning. RFID technology can be integrated into IoT systems for object tracking and management, ensuring seamless integration without any pervasiveness [25].

The rest of the paper is divided and organized into the following sections. Section II describes previous works on RFID-based digital twin systems and similar use cases of EM fingerprinting, solidifying its position as an identification key in a digital twin resolver. Section III describes a design for the resolver and associate network. Section IV presents evidence towards the successful implementation of EM fingerprinting in a digital twin resolver environment. The results are discussed in Section V and conclusions about the hypothetical digital twin resolver are drawn in Section VI.

II. Related Work

RFID tags have been employed in both the existing digital twin and modeled digital twin. Azangoo [21] makes the use of RFID tags in the digital twin system. Pavatar, an industrial IoT system for ultra-high voltage converter station (UHVCS) management [20], where two RFID tags are utilized to detect the leakage based on different patterns of RSSI signal strength and phase variations. RFID tags have been utilized by [22] to model digital twins based on the UML class diagram in which RFID tags are utilized to trace objects on the factory floor. Maizi and Bendavid [23] implement available RFID, Wi-Fi, and software infrastructure on a pilot warehouse digital twin where the ceiling of the warehouse, product pallets, and forklifts are equipped with RFID tags as a means for identification and position estimation whereas [20] utilizes RFID tags to capture real-time data of items picked by customers which are implemented in DT prototype for apparel retail store.

Periaswamy et al. [24] showed that RFID tags had unique EM fingerprints compared to their counterfeit counterparts, which indicates that the cloning problem for digital twins will be avoided and a transferable and unique key can be generated from the EM fingerprint. Bertoncini et al. [26] also indicated that the EM fingerprint may differ due to the manufacturing process, not just EPC content, which further solidifies the notion of cloning prevention. Yang et al. [27] used a non-intrusive and easily implementable EM fingerprinting method to characterize user-device interactions with the help of time-varying unique EM patterns, each associated to the use pattern of a specific user. Remley [28] showed that this technique could be feasibly applied to WLAN devices.

Although RFID tags have been used in different DT models, this paper presents a holistic approach to the possible use of RFID tags in the DT system based on the electromagnetic fingerprint of each RFID tag based on the tag's EPC or identifier associated.

III. Digital Twin Resolver Infrastructure

The proposed resolver system consists of an accessing device with internal memory serving as a personal database for all devices owned on the consumer end (computer, smartphone, or any other smart device connected to the digital realm), a spectrum analyzer that collects RFID tag signal strength data in the frequency domain, a database containing multiple signal strength readings from every RFID tag associated with each digital object, and the digital twin resolver, which will be a machine learning model trained on the aforementioned database. The spectrum analyzer reads the signal from the tag and saves the signal strength in the decibel-milliwatt unit across the entire UHF RFID spectrum. This data is saved by the accessing device and sent to the machine learning model for classification.

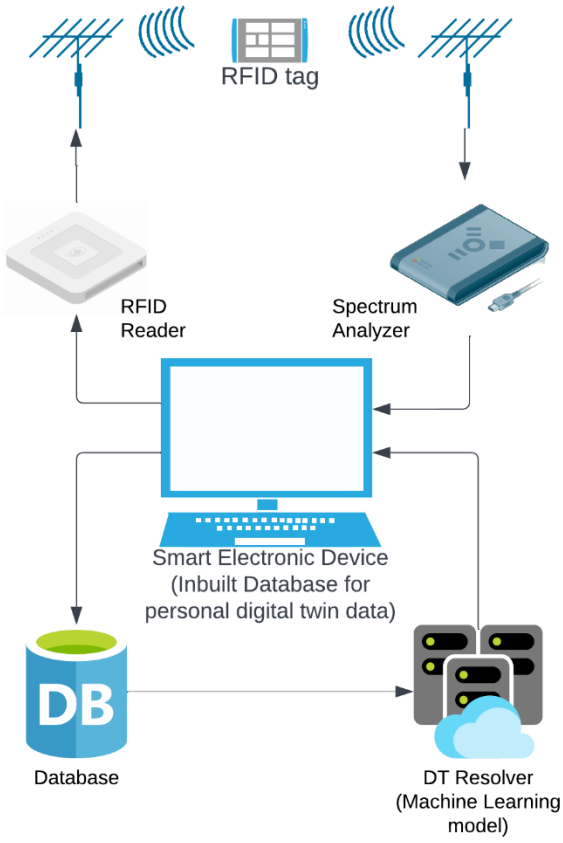


Fig. 1. Digital Twin Resolver Infrastructure Diagram

Once the algorithm matches the signal to its digital counterpart, the accessing device receives this information and assigns the identity to the new device or verifies the identity of a device with an existing digital twin. The model cannot be deceived by tag cloning because of the properties of an electromagnetic fingerprint signature obtained from an RFID tag [24]. This proposed system is shown in Figure 1. which includes an antenna attached to an RFID reader and spectrum analyzer to generate and read tag signal strength respectively.

This resolver will be able to address the following concerns associated with data-driven digital twins –

- Due to association of one RFID tag with an individually unique EM fingerprint, the resolver will be able to universally identify everything without any duplicate errors. No two EM fingerprints will be the same thus, ownership conflicts will not arise and each fingerprint resolves to one object only.
- Owner authentication will be based on data stored in local servers. The machine learning model will be able to classify specific fingerprints without error, enabling perfect authentication. The ownership transfer will automatically happen once the fingerprint enters a new user database after permission from the previous owner has been granted. This will also be used to verify data and identities.
- Data protection and privacy are also achieved due to each RFID EM fingerprint providing data irrelevant to the object it resolves to.
- Passive UHF RFID tags are low-cost and battery-free products, thus they are also scalable to any degree and can be used universally for all objects. These tags are versatile and can be used in other applications such as localization and supply chain management in conjunction with providing EM fingerprints.

TABLE I. TAG SPECIFICATIONS

	Beontag A61F [29]	Confidex Carrier Classic [30]
Air Interface Protocol:	EPCglobal UHF Class 1 Gen 2 (ISO 18000-63)	EPCglobal UHF Class 1 Gen 2 (ISO 18000-6C)
Operating Frequency:	Global (860-960 MHz)	Global (860-960 MHz)
IC Type:	Monza R6-P	Impinj Monza 4QT™
Memory:	EPC 128/96 bits, User 32/64 bits, TID 96 bits	EPC 128 bit, User 512 bit, TID 96 bit
EPC Memory Content:	Unique, auto-serialized	Not guaranteed unique
Applicable Surface Materials:	Wood, plastic, cardboard, rubber, cotton tissue, denim	Non-metallic surfaces
Operating Temperature:	-40° to +85°C (-40° to +185°F)	-35° to +85°C (-31° to +185°F)

IV. PROOF OF CONCEPT

To gather preliminary evidence towards the effectiveness of RFID tag electromagnetic fingerprinting, frequency domain signal strength data was gathered from 4 different RFID tags. Two of these tags were Beontag A61F RFID Paper Tags [29], and the other two were Confidex Classic Carrier RFID tags [30].

From an initial inspection the tag specifications as seen on Table I, the Confidex tags have higher user memory bank (512 bits) compared to Beontag (32 bits), as well as running different chips. The only similarity between the two tags is the EPC memory (128 bits). The EPC memory of each tag of any one of these manufacturers was filled with two different types of data. The first EPC was a mix of different numbers and characters – 300833B2DDD9014000000001, which was referred to as Type 1. The other EPC was a single digit preceded by zeros – 00000000000000000000000002, being referred to as Type 2. This covers any possible EPC conventions for industrial or universal use to assign to digital twins. As shown in Figure 2, for the case of Beontag tags, the signals have slight but distinct differences across the different EPCs. A machine learning model can further determine these differences and would be able to classify tags according to EPC data, laying the foundation for a Passive UHF RFID EM fingerprint based digital twin resolver.

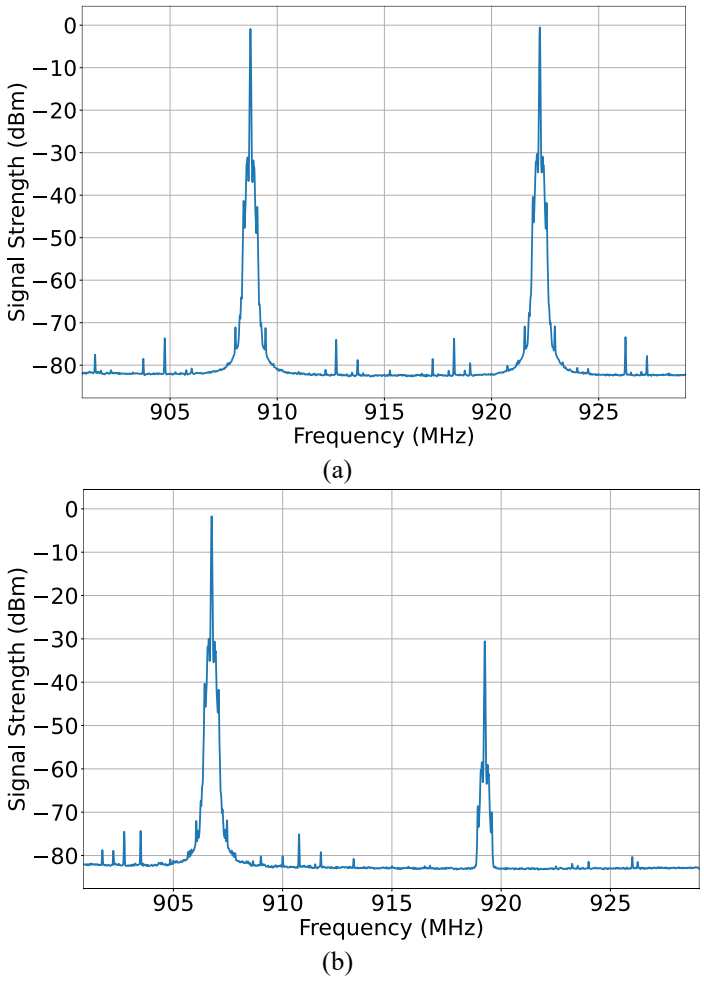


Fig. 2. Signal Strength vs. Frequency data obtained from spectrum analyzer for Beontag tags with (a) EPC Type 1 (b) EPC Type 2

As described in the previous section, data was generated using a RFID reader connected to an antenna that excited the RFID tags. The tag reply signal was captured by a spectrum analyzer in the entire UHF RFID spectrum. There were 4 tags, 2 Confidex tags with both aforementioned EPC types, and 2 Beontag tags with the same EPC types. Data collected from each tag is shown hypothetically in Table 2, each such file has 2 columns representing the axes and 4001 points representing the columns. For each tag, 100 signal strength readings were taken in the dBm (decibell milliwatt) unit. All of the classified data was then divided into two subsets – training and testing data. The training dataset was used to train the machine learning model and the testing dataset was used to evaluate the trained model. While training the machine learning model, only the EPC content of the tags was considered to be the target, the tag manufacturer was not a factor in making this distinction. It was not considered as a feature for the training of the model. But, this feature was used to make further subsets based on manufacturer to evaluate the performance of different types of tags. The machine learning model emulates the resolver of the described prototype.

TABLE II. SAMPLE DATA FROM SPECTRUM ANALYZER READING

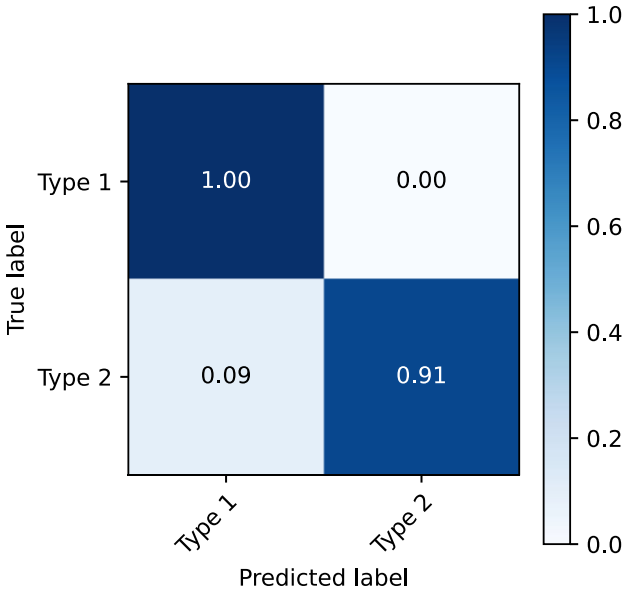
Frequency (MHz)	**dBm**
899.99	-99.53
900.00	-98.99
…	…
…	…
929.99	-97.68
930.00	-100.02

V. RESULTS

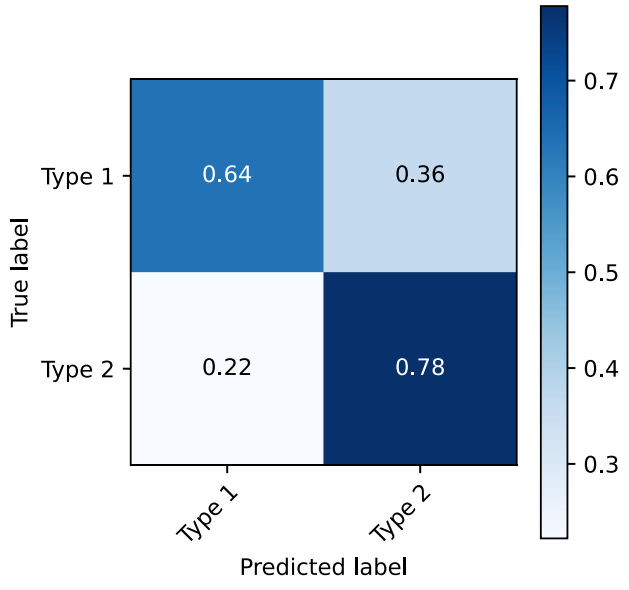
The XGBoost model was trained using 100 observations of each of the four tags. During the evaluation, the test data was split into Beontag and Confidex tag observations. The trained model was 100% accurate on the training data of both types of tags in terms of EPC detection. However, the model was able to differentiate EPC content of Beontag tags 95% of the time for test data, while it was able to do so only 55% of the time for the Confidex tags. Figure 2 shows that the model failed to detect the second type of EPC in the Confidex tag.

VI. CONCLUSION

The predictions obtained from the XGBoost model show that the tag with relatively inferior specifications showed more unique detectable characteristics across different EPCs. This variance may occur due to manufacturers implementing certain aspects of the LLRP protocol for specific use cases the tags are designed for while maintaining industry requirements and standards, similar to the implementation of Bluetooth protocol in wearable Bluetooth devices [31]. This indicates that the Beontag tags are suitable for the EM fingerprint digital twin resolver system since these tags exhibit more variable behavior across different units and EPC data, which may be due to less allocation in overall memory, meaning less data transmission within the used spectrum, minimizing congestion of variation in the signal read by the spectrum analyzer. Larger datasets are likely to result in a more accurate model. However, preliminary results are promising, with 99% overall accuracy for the Beontag tags. To further improve upon this, EM fingerprinting for electronic devices may also be a more effective idea to use as a key to its digital twin. The RFID signal may further add to the uniqueness of the device, making cloning impossible. Future work includes fleshing out the resolver in terms of ownership management and security measures to protect data stored in central and personal databases by implementing an encryption protocol.



(a)



(b)

Fig. 3. Normalized Confusion Matrices for EM fingerprint identification (a) Beontag tags (b) Confidex Tags

References

[1] M. Liu, S. Fang, H. Dong, and C. Xu, "Review of digital twin about concepts, technologies, and industrial applications," *J. Manuf. Syst.*, vol. 58, pp. 346–361, 2021.

[2] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary perspectives on complex systems*, Springer, 2017, pp. 85–113.

[3] F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Inform.*, vol. 15, no. 4, pp. 2405–2415, 2018.

[4] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108952–108971, 2020.

[5] R. Minerva, G. M. Lee, and N. Crespi, "Digital twin in the IoT context: a survey on technical features, scenarios, and architectural models," *Proc. IEEE*, vol. 108, no. 10, pp. 1785–1824, 2020.

[6] M. J. Kaur, V. P. Mishra, and P. Maheshwari, "The convergence of digital twin, IoT, and machine learning: transforming data into action," in *Digital twin technologies and smart cities*, Springer, 2020, pp. 3–17.

[7] A. Madni, C. Madni, and S. Lucero, "Leveraging Digital Twin Technology in Model-Based Systems Engineering," *Systems*, vol. 7, no. 1, p. 7, Jan. 2019, doi: 10.3390/systems7010007.

[8] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group*. Forschungsunion, 2013.

[9] Z. Liu, A. Zhang, and W. Wang, "A framework for an indoor safety management system based on digital twin," *Sensors*, vol. 20, no. 20, p. 5771, 2020.

[10] H. Huang, L. Yang, Y. Wang, X. Xu, and Y. Lu, "Digital Twin-driven online anomaly detection for an automation system based on edge intelligence," *J. Manuf. Syst.*, vol. 59, pp. 138–150, 2021.

[11] A. Z. Abideen, V. P. K. Sundram, J. Pyeman, A. K. Othman, and S. Sorooshian, "Digital twin integrated reinforced learning in supply chain and logistics," *Logistics*, vol. 5, no. 4, p. 84, 2021.

[12] F. Jaensch, A. Csiszar, C. Scheifele, and A. Verl, "Digital twins of manufacturing systems as a base for machine learning," in *2018 25th International Conference on Mechatronics and Machine Vision in Practice (M2VIP)*, 2018, pp. 1–6.

[13] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *Ieee Access*, vol. 8, pp. 21980–22012, 2020.

[14] S. M. N. Hasnaeen and A. Chrysler, "Detection of Malware in UHF RFID User Memory Bank using Random Forest Classifier on Signal Strength Data in the Frequency Domain," in *2022 IEEE International Conference on RFID (RFID)*, 2022, pp. 47–52.

[15] Y. L. dos Santos and E. Dias Canedo, "On the design and implementation of an IoT based architecture for reading ultra high frequency tags," *Information*, vol. 10, no. 2, p. 41, 2019.

[16] B. Durtschi, M. Mahat, M. Mashal, and A. Chrysler, "Preliminary Analysis of RFID Localization System for Moving Precast Concrete Units using Multiple-Tags and Weighted Euclid Distance k-NN algorithm," in *2021 IEEE International Conference on RFID (RFID)*, 2021, pp. 1–8.

[17] P. N. Tran and N. Boukhatem, "IP-based RFID architecture and location management," in *2008 16th International Conference on Software, Telecommunications and Computer Networks*, 2008, pp. 95–99.

[18] "Electronic Product Codes (EPCs) - Explained - The Business Professor, LLC." https://thebusinessprofessor.com/en_US/mgmt-operations/electronic-product-codes-epcs-explained (accessed Jul. 29, 2022).

[19] J. Guo *et al.*, "Tagleak: Non-intrusive and battery-free liquid leakage detection with backscattered signals," in *2018 IEEE International Conference on Industrial Internet (ICII)*, 2018, pp. 40–48.

[20] "Pavatar - Digital Twin for Industrial IoTs." http://tns.thss.tsinghua.edu.cn/sun/pavatar.html (accessed Jul. 21, 2022).

[21] M. Azangoo, A. Taherkordi, and J. O. Blech, "Digital twins for manufacturing using UML and behavioral specifications," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2020, vol. 1, pp. 1035–1038.

[22] M. Braglia, R. Gabbrielli, M. Frosolini, L. Marrazzini, and L. Padellini, "Using RFID technology and Discrete-Events, Agent-Based simulation tools to build Digital-Twins of large warehouses," in *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 2019, pp. 464–469.

[23] Y. Maïzi and Y. Bendavid, "Building a digital twin for IoT smart stores: A case in retail and apparel industry," *Int. J. Simul. Process Model.*, vol. 16, no. 2, pp. 147–160, 2021.

[24] S. C. G. Periaswamy, D. R. Thompson, and Jia Di, "Fingerprinting RFID Tags," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 938–943, Nov. 2011, doi: 10.1109/TDSC.2010.56.

[25] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks," *Sensors*, vol. 20, no. 9, p. 2495, Apr. 2020, doi: 10.3390/s20092495.

[26] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (RFID) tags," *IEEE Trans. Ind. Electron.*, vol. 59, no. 12, pp. 4843–4850, 2011.

[27] L. Yang *et al.*, "Magprint: Deep learning based user fingerprinting using electromagnetic signals," in *IEEE*

INFOCOM 2020-IEEE Conference on Computer Communications, 2020, pp. 696–705.

[28] K. A. Remley *et al.*, "Electromagnetic signatures of WLAN cards and network security," in *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.*, 2005, pp. 484–488.

[29] "Beontag A61F RFID Paper Tag (Monza R6-P)," *atlasRFIDstore*. https://www.atlasrfidstore.com/beontag-a61f-rfid-paper-tag-monza-r6-p/ (accessed Jul. 21, 2022).

[30] "Confidex Carrier Classic™ RFID Tag," *atlasRFIDstore*. https://www.atlasrfidstore.com/confidex-carrier-classic-rfid-tag/ (accessed Jul. 21, 2022).

[31] H. Aksu, A. S. Uluagac, and E. S. Bentley, "Identification of wearable devices with bluetooth," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 2, pp. 221–230, 2018.