Virtualized Controller for Computational RFID-based IoT Sensors in Industry 4.0

A
Dissertation
Presented to
the faculty of the School of Engineering and Applied Science
University of Virginia

---

in partial fulfillment
of the requirements for the degree

Doctor of Philosophy in Electrical Engineering

by

Rocio Elisa Pantoja Rodriguez

May 2024

APPROVAL SHEET

This

Dissertation

is submitted in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy

Author: Rocio Elisa Pantoja Rodriguez

This Dissertation has been read and approved by the examing committee:

Advisor: Mircea R. Stan

Advisor:

Committee Member: Brad Campbell

Committee Member: Sarah Sun

Committee Member: Steven M. Bowers

Committee Member: Robert Klenke

Committee Member:

Committee Member:

Accepted for the School of Engineering and Applied Science:

Jennifer L. West, School of Engineering and Applied Science

May 2024

To my dear family and friends.

"... for the soul becomes dyed with the color of its thoughts."

— Marcus Aurelius, Meditations

Abstract

RFID technology is ubiquitous in business and industrial operations, access security, and identification methods. With the advent of Computational RFID (CRFID), microcontrollers integrated into RFID tags add computational capabilities that enable broader adoption in the IoT. However, the challenge CRFID encounters is optimizing power distribution and consumption across the billions of IoT devices expected in the coming years. This dissertation explores approaches to balance RF energy harvesting and minimize power consumption in RFID-based IoT devices, addressing the crucial issue of battery limitations in terms of lifetime and maintenance. We focus on enhancing sensor tags beyond the role of simple data collectors into intelligent systems that utilize RF for sensing, computing, and self-power. The approach proposed reaches back to the core aspects of RFID and preserves the simplicity of RFID tags, shifting computational tasks from the tag microcontroller onto the reader to optimize tag resources. We implement a virtualized controller for SPI-over-RF (VCRFID), enabling the transmission of wireless SPI control instructions from the reader to embedded sensors on tags via the RF chip. We explore the development of a reader's firmware capable of handling custom RF SPI commands, creating a framework for the research, design, and fabrication of CRFID prototypes. Our research demonstrated that VCRFID sensing devices eliminate the need for a microcontroller and its associated power requirements, achieving

a 97% reduction in energy consumption compared to tags with MCUs. With the proposed RF harvester sensitivity of -31.4 dBm and a power conversion efficiency of 31.3%, longer-range operations would extend the VCRFID's reach beyond the initially reported distance. We completed and analyzed the integration of the VCRFID system from an edge-powered wireless sensor network to a cloud platform. The combination of VCRFID sensing technology and machine learning methods promises to advance the capabilities of RFID-based wireless IoT sensors for predictive maintenance applications in Industry 4.0.

Acknowledgments

I extend my deepest gratitude to my advisor, Professor Mircea Stan, for his invaluable and appreciated guidance on the non-deterministic road that research is. Professor Stan has stood by us through the most challenging times at UVA. With his understanding and care, his lead has been pivotal in our projects, with a keen emphasis on innovation and always keeping us focused on the best approach to the problem, particularly when we have been stuck trying to find a practical solution.

I am equally grateful to my Dissertation Thesis Committee members: Prof. Brad Campbell for his invaluable assistance with the IoT aspects of our project and for imparting his knowledge on cloud integration; Prof. Steve Bowers, Prof. Sarah Sun, and Prof. Robert Klenke for their insightful suggestions and feedback. Their expertise and dedication to research and teaching have been a source of inspiration and motivation. A special thank you goes to Beth A. Eastwood-Beatty, our Graduate Coordinator, whose efforts keep the heart of the ECE department beating. Also, thanks to the members of Link Lab for being a center of collaboration and learning.

Thank you to my peers and friends at UVA, both within the HPLP group and beyond. My dear

friends, you have been vital in my success, and I have learned the true meaning of community. I am grateful to you and your families; witnessing our collective growth has been a joy. I extend my appreciation to my fellow female graduate students at the School of Engineering and Applied Sciences and GradSWE, advocating for diversity and inclusion in spaces where women continue to be minorities.

Moreover, I dedicate my work to my parents, whose relentless hard work and sacrifice have sought to provide me with the best education and set a stellar example of dedication. *Gracias Ma por tu apoyo constante y por creer siempre en mi.* A thanks go to my aunts and uncles for broadening my horizons with your example. I offer my prayers to the memory of my elders, to my grandpa, who enlightened me with our talks on Latin expressions and Roman law; and to my dear grandma, our guide and the pillar of the family, whose recent parting to God's side hurts so much. To my beloved husband, thank you for being a source of encouragement and a true companion, always listening to my ideas, finding the best side of the situation, and especially for being an amazing dad to our little baby. My dear child, you have made us know heaven on earth; all this is for you.

Contents

List of Figures

List of Tables

Chapter 1

Thesis

1.1 Introduction

The 21st century has witnessed the advent of the Internet of Things (IoT), where everyday physical objects form part of a smart, interconnected network of devices. Wireless technologies are crucial in facilitating this development by allowing wireless communication [1, 2], control [3], monitoring [4], and automation [5] without physical connections, being unplugged but connected [1]. For example, the smartphones we rely on daily are powerful computers that allow us not only to communicate from anywhere and connect with any point of the world but, when used to pay with a tap, have come to replace physical cash and cards [6, 7]. Undoubtedly, the demand for connectivity and information about our world drives steadfastly this century's digital cyber-physical revolution.

Following Moore's Law, the increase in transistor density over time has overcome the limitations

silicon faces at the atomic scale and facilitates the development of more powerful and efficient devices capable of supporting an extensive range of applications. At the same time, the rising demand for these devices drives the expansion of the number of personal computing and IoT devices globally. This expansion poses significant challenges in optimizing energy consumption and power distribution across the billions of devices expected to be deployed in the coming years. This challenge is not only about ensuring that these devices can operate efficiently on minimal power but also about reducing the overall energy footprint of the expanding digital ecosystem. Addressing these issues requires innovative approaches in circuit design and system architecture, alongside the development of better energy harvesters, low-power protocols, and smart power management techniques.

Together with WiFi, cellular networks, and Bluetooth, Radio Frequency Identification (RFID) is a wireless passive technology that has gained widespread adoption in our daily lives. RFID is present in our phone's NFC and in the cards we use to pay or as a means of entry into buildings. RFID is favored for its low cost, ability to communicate purely on the received power from the transmitter, ultra-low power consumption, and simplicity [8]. For these reasons, RFID is extensively used in the supply chain and is particularly well-suited for applications in Industry 4.0. This passive technology plays a crucial role in tagging, tracking, and inventorying assets [9]. However, despite the progress in ultra-low-power computational elements such as microcontrollers and system-on-chip, CRFID still faces limited computational resources, a reduced power capacity, and a dependence on batteries for power-intensive applications, which hinder a broader adoption.

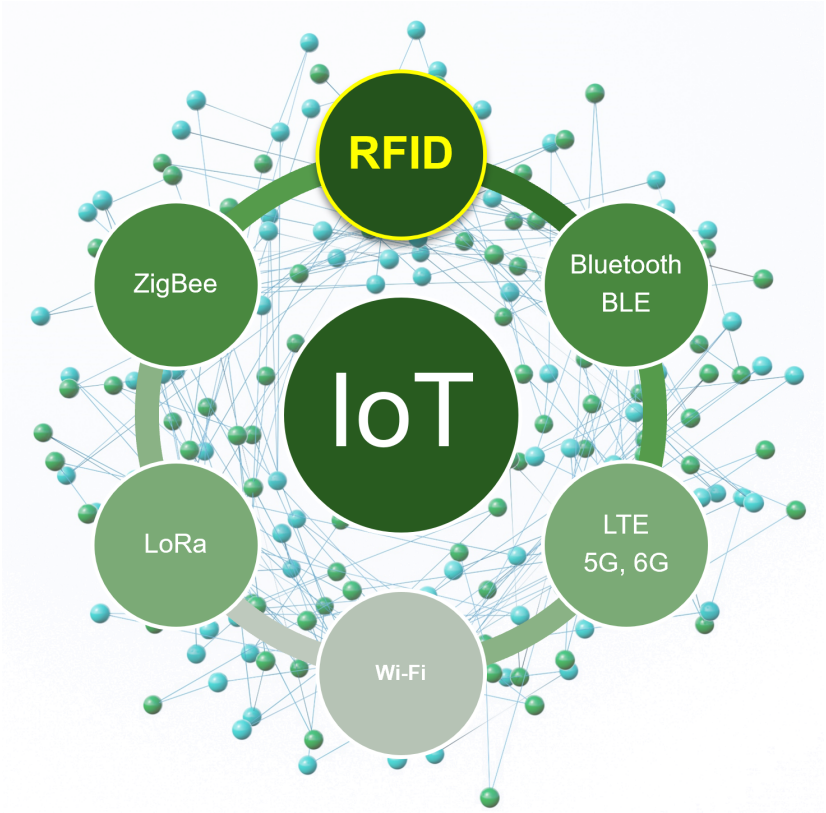

Figure 1.1: IoT wireless technologies include WiFi, cellular networks, LoRa, Bluetooth, and, although ubiquitous, the less referenced Radio Frequency Identification (RFID).

Compared to the RFID market, which was estimated at USD 10.7 billion in 2021 [11], the global IoT market will reach around USD 336 billion in 2024, with projections indicating a nearly 6-fold increase over a decade [12]. This highlights the importance of IoT applications and their critical role in modern technology, with the most important segment in IoT being consumer devices such as smartphones. The total number of IoT devices is expected to reach over 17 billion in 2024, surpassing by twofold the number of people on Earth [10]; in China alone, the number of IoT devices is estimated to reach 8 billion by 2030 [13].

We are looking at a future Trillion IoT devices market [14], making every challenge we face even

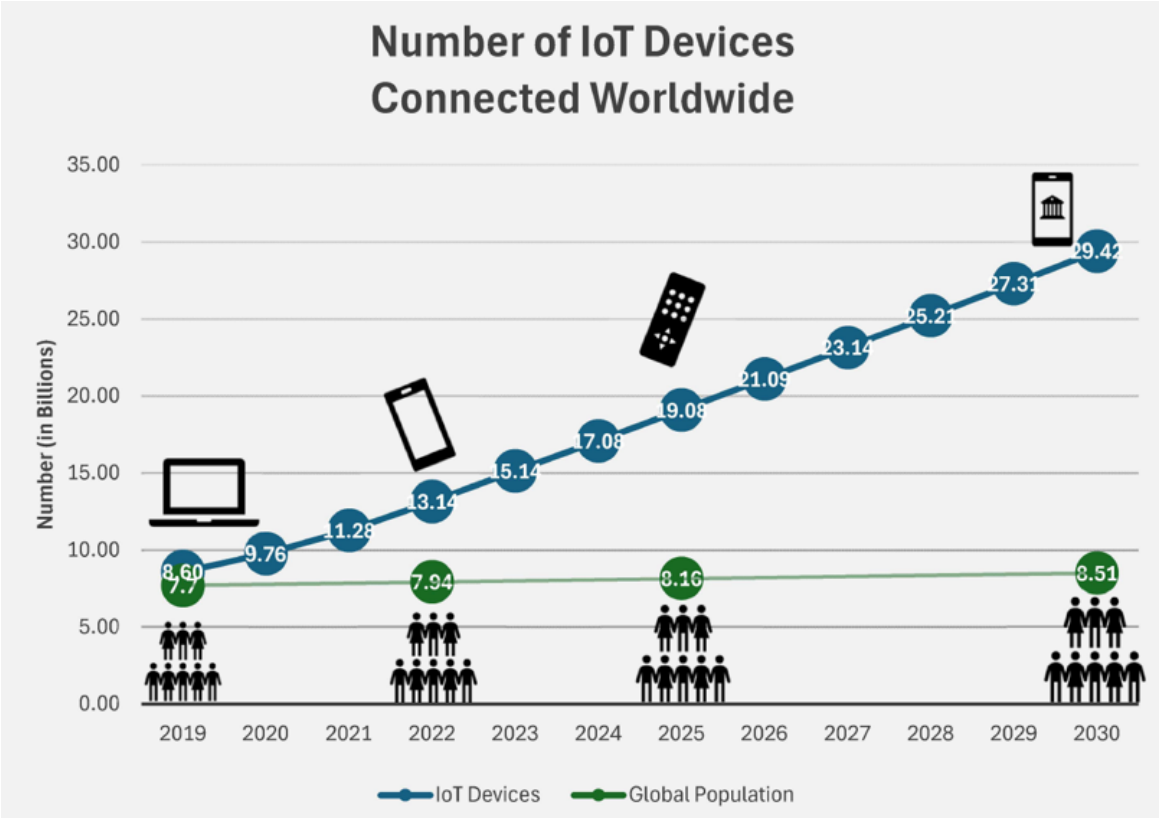

Figure 1.2: The total number of IoT devices is expected to reach over 17 billion in 2024, surpassing by twofold the number of people on Earth (data adapted from [10]).

larger by scale. Conventional power sources, such as batteries and wired power, become unsustainable and impractical at the scale of billions or trillions of devices [15, 16]. The limitations of batteries contribute to increased costs and heightened maintenance demands. At the same time, the reliance on power wires significantly hinders the wireless capabilities of these devices, representing a persistent challenge that restricts the application of technology [17].

Furthermore, as transmitted power is a limited resource, achieving efficiency and low power consumption at the receiver device is paramount. The 915 MHz frequency band generally has better propagation characteristics compared to 2.45 GHz. Lower frequencies experience less attenuation

in free space, leading to better propagation. Both frequency bands are influenced by the inverse square law, where power density decreases with the square of the distance from the source. Given equal output power (1 W), the transmission at 915 MHz is expected to result in a slightly higher power density.

For instance, a theoretical estimate of RF power in the μW range is available at a distance of a few meters from an RFID reader transmitting at 1 W; highlighting the need for solutions towards attaining higher sensitivity, larger efficiency, and better resource utilization [18].

In this context, we analyze the impact of power consumption and explore the potential of an RF sensing system under the constraints of the energy source. We can analyze the relationship between the transmitted power, the distance between transmitter and receiver, and the efficiency of the energy harvesting system. A fundamental approach is to employ the Friis transmission formula:

$$P_R = \frac{P_T G_T G_R \lambda^2}{(4\pi d)^2}$$

where:

- P_R is the RF power received,
- P_T is the RF power transmitted,
- G_T and G_R are the transmitter and receiver antenna gains, respectively,
- λ is the wavelength of the transmitted signal,

- d is the range or the distance from the transmitter to the receiver antenna.

To account for losses occurring at each of the stages associated with antenna matching and rectification, we express them in a single efficiency constant η with values between 0 and 1, where 1 would mean 100% efficient conversion with no losses. The received DC power (P_{DC}) by the RFID tag is then given by:

$$P_{DC} = \eta P_R$$

we can express the DC power received from the initial RF power as:

$$P_{DC} = \eta \frac{P_T G_T G_R \lambda^2}{(4\pi r)^2}$$

To ensure the feasibility of powering a particular workload with the received power at the tag over the specific distance d, the required power, P_{REQ}, can be stated as:

$$P_{\text{REQ}} \leq P_{\text{DC}} = \eta \frac{P_{\text{T}} G_{\text{T}} G_{\text{R}} \lambda^2}{(4\pi d)^2}$$

A reduction in power requirements is the result of the application of direct power improvement techniques, indicating a more efficient consumption of energy-critical system components. Such reduced power can be achieved partially, for example, by reduction of the operational frequency of a sensing device's microcontroller. We suggest that the virtualization of functions instead of

executing them on an embedded microprocessor can significantly reduce the device's required power. With this analysis, we can better understand the parameters that govern the efficacy of RF energy transfer and, consequently, devise more efficient sensing systems that align with the constraints of our energy resources. Another critical issue arising from the rapid expansion in the number of sensors is that the growth rate in data generated exceeds our capacity to harness and process it intelligently. With the number of sensors estimated to be $>$45 trillion in 2032, it is also estimated that the devices will generate $>$1 million zettabytes of data per year [14]. Transmitting and storing such massive amounts of data is costly and inefficient, as it consumes a lot of energy and bandwidth. With this in mind, we seek options to harness data and process the data closer to where it's been generated, i.e., with edge devices.

Moreover, robust security measures are essential to prevent and detect tampering, maintain access control, and protect the wireless exchange of data, ensuring that the data we transmit is private and secure and that it cannot be intercepted, modified, or duplicated [19].

With computational RFID tags, and to alleviate the challenge of delivering power, we seek to achieve a balance between maximizing harvested RF and decreasing consumed power. The first can be achieved by reducing RF losses with a design with a higher-sensitivity RF rectifier and peak power conversion efficiency (PCE). The second can be achieved by using ultra-low-power ICs and targeting the reduction of elements that consume power. In this work, we suggest an alternative way of controlling the sensors wirelessly, eliminating onboard microcontrollers on the RFID tags when possible, achieving a substantial required power reduction. This work presents an innovative approach to wireless industrial IoT devices based on computational RFID technology that merges

the best of long-established ubiquitous RFID with the computational and sensing capabilities of newer technologies.

1.1.1 VCRFID for IoT Sensing Applications

Smart monitoring devices observe changes in real time and learn from historical machine behavior, actively preventing industrial equipment failures by anticipating them. Deloitte's reports indicate that the use of predictive maintenance techniques can cut downtime by 15%, boost industrial productivity by up to 20%, and reduce the need for spare equipment parts by up to 30% [20]. Due to these benefits, the market interest in predictive maintenance is estimated to rise to between $4-6 billion USD and, in the next ten years, will reach several tens of billions. [21, 22].

The research presented in this thesis introduces a computational RFID system expected to be adopted for remote equipment monitoring applications. Predictive maintenance enables proactive actions to prevent machine failures, saving time and reducing costs. Adopting the Industrial Internet of Things (IIoT) enhances business efficiency and better decision-making based on real data. IIoT transcends beyond merely keeping pace with technology and contributes to improving operational processes, how the work is planned, and towards a more sustainable and competitive future [20].

1.2 Thesis Statement

A Virtualized Computational RFID system can enable wireless self-powered sensors with improved power utilization efficiency by off-loading resource-intensive tasks to the reader.

Moreover, sensor data can be used to detect anomalies in predictive maintenance applications through the VCRFID edge-to-cloud integration with ML methods. Simultaneously, the VCRFID system acts as a framework that enables the research, design, and development of new CRFID prototypes for wireless sensing.

1.2.1 Elaboration

The thesis statement highlights the novel VCRFID system as the focal point of our research. The VCRFID system enables the research and development of new CRFID prototypes without batteries or wired power for wireless sensing through a virtualized interface. Computational RFID is based on RFID technology and uses electromagnetic fields to identify objects with tags attached to them. The tag or sensor communicates identity information and possesses computational power to process data or execute tasks such as sensing. In this context, virtualization refers to the virtualization of the interface into a new controlling type. Combining RFID technology, computational capabilities, and sensing enhances RFID functionality beyond identification and tracking functions.

The sensors embedded in the RFID tag obtain power through energy harvesting methods, converting RF energy from the environment into electrical energy. This is where a highly sensitive receiver is key for the application. The further from the source, the harder it is for the devices

to harvest power from the incidental RF. Power Utilization Efficiency looks at the effectiveness with which a device uses power to perform its intended tasks. Improving this efficiency means the device operates with less wasted energy, which is particularly important for energy-harvesting devices.

Resource-intensive tasks that require significant computational power or energy are handled by the reader, who is typically more capable and less constrained by power limitations. The Edge-to-Cloud Integration is the system architecture that allows data to flow from the edge of the network, where the sensors and readers are located, to cloud-based services for further processing and analysis. This approach addresses the 'data deluge' problem by enabling the selective transmission of only significant data points. By filtering out the data at the edge, it reduces the volume of data sent to the cloud, enhancing efficiency and focusing processing resources on key information.

In addition, detecting anomalies is crucial for applications such as predictive maintenance. ML methods on the data collected by the VCRFID sensor systems allow for intervention before costly breakdowns occur based on unusual patterns or outliers in data detected that could indicate a deviation from expected behavior.

The framework for the virtualized computational RFID system provides a way to build, deploy, and operate applications, including tools for developing new Computational RFID prototypes, a basis for further development of CRFID technology.

1.3 Contributions

In this thesis, we seek to enhance RFID tags beyond their role as data collectors into intelligent autonomous systems that utilize RF for sensing, computing, and self-power. We reach back to the core essence of RFID and keep the smart tags as simple as possible by moving heavier computational tasks onto the reader, keeping the tags as low-cost devices that are easy to implement in multiple scenarios. In the proposed system, RFID tags are utilized to establish a sensor network that enables real-time accessibility of the data captured by these tags from any location through the data visualization tools. This dissertation's main contributions are the following:

1. The design and fabrication of a new type of ultra-low power sensing tags, where the innovation is achieved through a microcontroller-free design approach, combining UHF RF energy harvesting and sensor integration into an energy-efficient battery-less sensing RFID tag design for the VCRFID system.

2. The development of new reader applications and firmware based on the ST25Ru3993 board from STMicroelectronics as the reader hardware of the VCRFID sensor system. The firmware supports the EPC-Global Class 1 Gen-2 UHF RFID Standard, which establishes a virtualized controller for SPI-over-RF, enabling seamless communication and control over the tag devices. The system integrates RF energy harvesting and wireless sensor control, increasing efficiency and expanding the scope of RFID technology in sensing applications.

3. The implementation of Wireless Sensor Networks (WSN) with edge data processing reduces latency and minimizes transmission costs in a sensor-to-cloud architecture. This approach

keeps data in proximity to its source, reducing transmission costs and delays in real-time anomaly detection applications.

4. The combination of the VCRFID system with machine learning techniques for conducting ML analysis, specifically targeting temperature sensing applications aimed at remote monitoring and applications oriented to equipment predictive maintenance.

5. We introduce an enhanced RDR RF harvester design with a sensitivity of -31.4 dBm and a power conversion efficiency of 31.3%.The proposed design enables longer-range operations that could significantly increase the operational reach of the VCRFID system beyond previously reported distances.

6. A framework for the research, design, and development of CRFID prototypes that can be extended beyond Industry 4.0 scenarios. It includes a suite of development tools and libraries to streamline the design, testing, and creation of new applications. Additionally, the framework supports iterative optimization processes, ensuring compatibility and functionality across various hardware platforms.

Chapter 2

Background on RFID

2.1 RFID Technology

Radio-frequency identification (RFID) is a wireless technology based on using electromagnetic waves for communication, primarily used for the identification and tracking of tagged objects [23]. Beyond its origins with Walmart's retail supply chain and the Department of Defense's military suppliers, RFID has found itself pervasive in applications such as keyless access control, automatic toll collection systems, apparel retail, and animal and people tracking. RFID systems' ability to generate vast amounts of data on item movements, interactions, and locations presents a significant opportunity for advanced data analytics and AI algorithms to extract meaningful insights, predict trends, and optimize operations.

The two most essential components of an RFID system are a transponder or RFID tag and an interrogator, also called a reader device [8]. Fig 2.1 presents a diagram of a standard UHF RFID system. This system includes a computer that oversees the operation of an RFID reader. The reader is responsible for handling the transmitting and receiving radio frequency (RF) signals via the antenna. The RFID tag replies by modulating the RF energy emitted by the antenna.

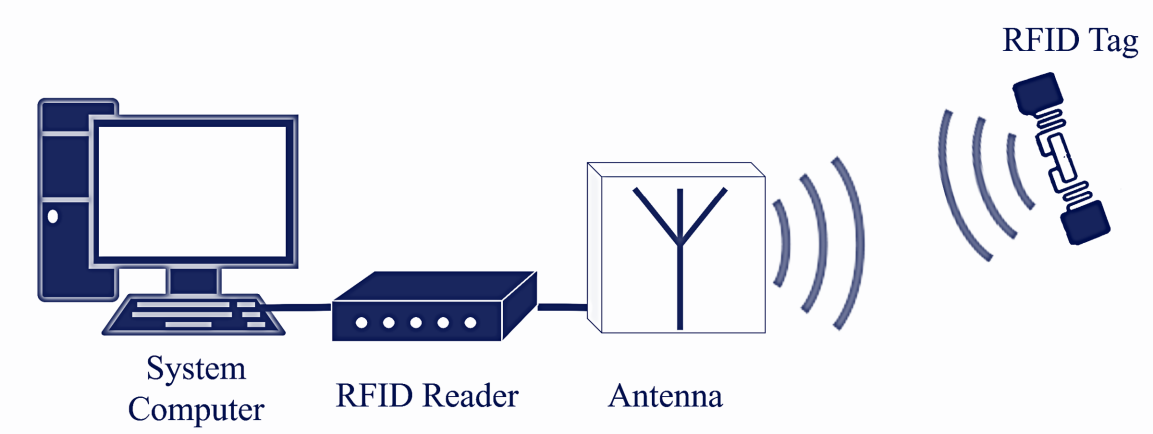

Figure 2.1: Diagram of a basic UHF RFID system. The UHF RFID system comprises a reader that sends and receives signals from the antenna. The RFID tag reflects the signal with a modulated response. The received RF energy powers the chip on the RFID tag.

2.1.1 RFID Tags

An RFID tag is an intelligent label device enabled to communicate with a reader via radio frequency (RF) signals. The RFID tag primary function is to store and transmit data about the tagged object [8]. Generally, it comprises two elements: an antenna and a microchip mounted on a plastic substrate. RFID tags come in various form factors, determined by the antenna type and frequency used to match specific applications.

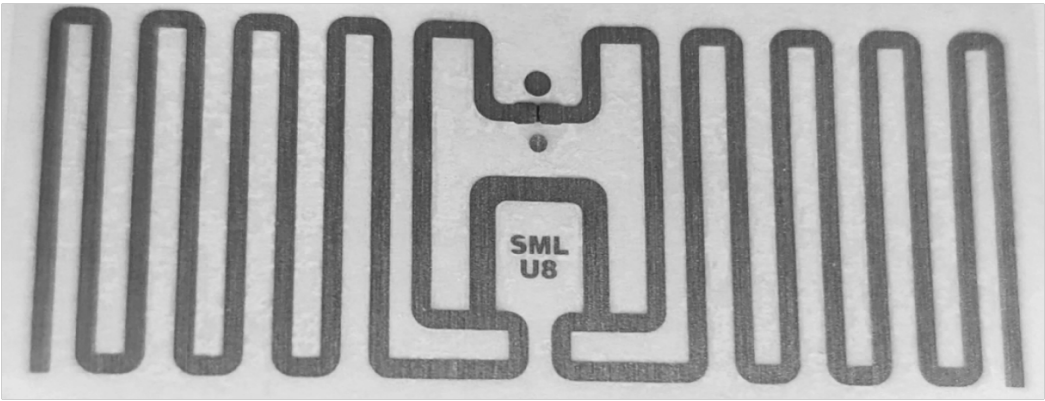

Figure 2.2: Picture of a commercial UHF RFID tag. The passive UHF RFID tag shown consists of an antenna and an RFID chip.

RFID Tags Taxonomy: Passive, Active, and BAP Tags

A **passive** RFID tag operates without a self-contained power source, such as a battery. Instead, when the RFID reader emits a radio signal, the tag's antenna captures the electromagnetic signal, inducing a current that powers the tag's RF chip. The absence of batteries keeps the cost and intricacy of passive RFID tags compared to their active RFID counterparts. In essence, passive RFID tags rely solely on the tag antenna RF backscattering to power the RF chip, simplifying their design and operation.

In contrast, **active** RFID tags are battery-operated. The added power supply allows active RFID tags to transmit signals actively rather than relying on incoming signals to induce power. The presence of a battery in active RFID tags provides several advantages, including longer read ranges and enhanced signal strength. However, it also increases cost and a limited lifespan due to the finite battery life.

Another class of RFID tags is the **Battery-Assisted Passive (BAP)** and **Pseudo-BAP** tags. These tags are a variation of the passive tags. BAP tags combine the benefits of active and passive tags. When a BAP tag receives an RF signal from an RFID reader, it uses an embedded battery to activate and power the RFID Tag IC within the tag. This enables BAP tags to respond more actively, improving read ranges and data reliability.

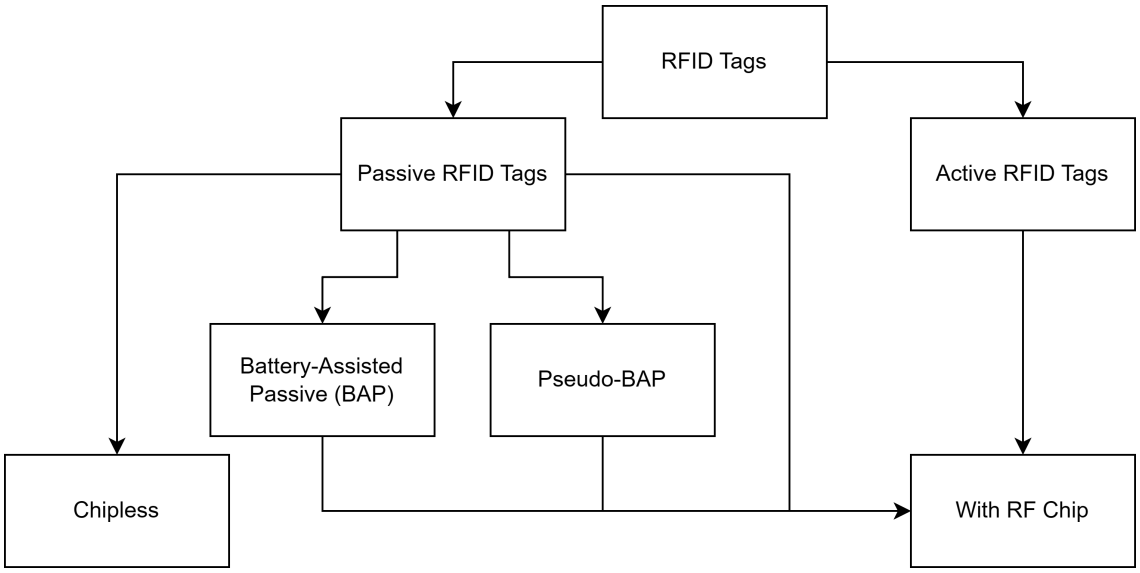

Figure 2.3: Taxonomy of UHF RFID tags based on power mode and chip or chipless type.

2.1.2 RFID Readers

An RFID reader is a device that manages sending and receiving radio signals to the RFID tag. The strength of the signal that the reader sends to the transmitting antenna is called the output power, and it is measured in dBm. Commercial UHF readers generally have a maximum output power of 30 dBm, regulated by FCC limitations. In some instances, that power is 33 dBm, which accounts for losses in the transmitting cables or antenna.

The logarithmic scale underscores that a loss of 3 dBm, i.e., going from 30 dBm to 27 dBm (equivalent to 1 W to 0.5 W), will result in a loss of 50% of the transmitted power, more evident when we compare the values expressed in watts.

Moreover, with the increased number of devices and wireless applications requiring reliable transmitted power, companies like Energous and Wiliot have sought approval from FCC for 15 W power transmitters, which enables even higher power transmission of RF-powered IoT devices at a distance [24]. The relevance of this relies on the fact that RF power decreases steeply with increasing distance from the source, obeying the inverse-square law of radio propagation [25]. This progressive decrease in power highlights the need for more robust transmission capabilities, particularly in environments where devices must operate over larger areas. Enhanced power transmitters could, therefore, provide a significant boost in the operational range and reliability of devices, opening the way for new applications. The advent of higher-power transmitter technologies could make it feasible for widespread use in everything from industrial sensors to consumer electronics.

As first introduced in the previous chapter, in RF systems, we can make use of the Friis Transmission equation (2.1) to calculate the power at a distance, d, from the transmitter [26].

In equation (2.1), the received power at the RFID tag (in watts), P_R, is expressed as:

$$P_R = \frac{P_T G_T G_R \lambda^2}{(4\pi d)^2 L} \tag{2.1}$$

Where:

P_T is the transmitted power in free space by the RFID tag reader (in watts)

G_T is the gain of the reader's transmitting antenna

G_T is the gain of the RFID tag's receiving antenna

λ is the wavelength of the RF signal (in meters)

d is the distance between the RFID tag and the reader (in meters).

L represents the path loss, accounting for absorption, reflection, and signal interference

This equation is particularly relevant for calculating the signal strength at the receiver point. In addition, it helps to understand the relationship between the parameters affecting the reading range of RFID tags.

Originating from Friis's work in 1946, this formula provides a mathematical model for estimating the power received by an antenna under idealized conditions. This equation assumes that the transmitted power is spread directed by the antenna's gain. Specifically, the formula calculates how the transmitted power from one antenna is received by another at a certain distance, factoring in the gain of both the transmitting and receiving antennas.

The underlying principle behind the Friis equation is that the power transmitted from an antenna disperses over a sphere as it travels through space. As the distance from the antenna increases, the surface area of this sphere expands, following the square of the radius—hence the inverse square law effect. Essentially, the power at any given point on the sphere's surface is the initial power divided by the area of the sphere. This explains why signal strength diminishes with increasing

distance between the transmitter and the receiver. The Friis equation provides a critical tool for optimizing wireless communication systems, as the ones shown in the following sections.

2.1.3 RF Communication and Frequencies

Data Rate

Data rates for RFID systems utilizing the UHF band at 915 MHz are notably higher than LF RFID. In contrast to the data rates of Kbps seen in LF RFID systems, UHF RFID systems achieve much faster communication speeds. The reason for this increase in data rate is closely tied to the frequency of operation. As the operating frequency rises, so do the bandwidth and data rates, reaching Mbps range at microwave frequencies. The data rates for UHF RFID systems can range from 40 Kbps to 27 Mbps.

RFID Frequencies

Table 2.1 lists the different RFID frequency bands in the electromagnetic spectrum used for RFID applications. This work will focus exclusively on the UHF band with a center frequency at 915 MHz.

Table 2.1: RFID Frequency Bands [8, 27]

Frequency Band	**Operating Frequency**	**Typical Applications**
Low Frequency (LF)	125-134 KHz	Access control, animal identification, proximity cards, low-range tracking
High Frequency (HF)	13.56 MHz	Smart cards, contactless payment, NFC
Ultra-High Frequency (UHF)	860-960 MHz	Logistics, inventory management, supply chain tracking, retail, asset tracking
Microwave (SHF)	2.45-30 GHz	Communication, radar, navigation, remote sensing, and medical treatment
Millimeter Wave (EHF)	24 GHz, 30 GHz and above	Specialized applications, scientific uses and communication data links

2.2 State of the Art: Evolution from RFID to CRFID

The capabilities of RFID tags have been enhanced by integrating microcontrollers, expanded memory, and sensors. This advancement has led to the rise of intelligent Computational RFIDs (CRFIDs), towards a battery-less and wireless IoT technology that enables innovative RFID applications in computing, telemetry, vision, and machine learning.

Previous research has explored the use of RFID tags for wireless sensing applications and made the first steps in creating platforms called Computational Radio Frequency Identification, CRFID. In the following sections, we highlight some of the most significant works exploring the sensing and computing capabilities of RFID tags, drawing from valuable insights gained through challenges faced and lessons learned. The use of the EPC-Global Class 1 Generation-2 UHF RFID interface protocol enables not only RF communication but also modulation, encoding, medium access schemes, and the use of custom RF commands to send instructions from the reader to embedded sensors on the RFID tags through the RF chip. We explore this in section 3 with the VCRFID system tags that use the EM4325 chip described next.

2.2.1 WISP

A trailblazer of the CRFID field is the Wireless Identification and Sensing Platform (WISP), a computational RFID system introduced by the University of Washington in collaboration with Intel [28, 29]. The WISP platform was one of the first to add a microcontroller to an RFID device. The Wireless Identification and Sensing Platform (WISP) was created with the purpose of measuring tag motion using long-range UHF RFID tags, which, until the creation of WISP, power constraints would make impossible on RFID the implementation of sensors or the use of a microcontroller [28]. π-WISP was one of the first RFID tags to detect motion. It used a TI MSP430 microcontroller powered by RF harvesting of a 915 MHz signal and three orthogonally mounted mercury switches working as a three-axis accelerometer [30]. Although the computational capabilities were improved with the MSP430 microcontroller, this ended up leading to increased current consumption and limited reading range. Based on the previous π-WISP device, a novel WISP architecture was developed using discrete components. The CRFID system tag was embedded with sensors that detect object motion running EPC C1G1 RFID protocol on the MSP430 microcontroller, which was used to establish communication with a reader [31]. Still an active project and available in the market, WISP continues its contributions to the field of wireless sensing platforms.

2.2.2 EM Microelectronic: EM4325 RF IC

The EPC-Global Class 1 Generation 2 EM4325 is a versatile RFID IC that operates as both a passive and battery-assisted passive RFID IC. There are previous works where RFID tag designs utilize the EM4325 IC developed by EM Microelectronic. The EM4325 RFID IC serves as both

passive and battery-assisted passive RFID IC, offering versatility. Various studies, including [32–35], have utilized RFID tags with the EM4325 IC for temperature measurements. Researchers built custom tag's antenna designs in each study to match their specific application needs, resulting in unique tag designs.

2.2.3 Farsens

Farsens is a company that fabricates RFID ICs and RFID sensors. They developed the ROCKY100 and ANDY100 IC UHF with RF communication, power harvesting, embedded temperature sensor, and a configurable SPI master module [36]. Beriain et al. [37] developed a battery-less RFID tag based on an ANDY100 IC by Farsens, which includes UHF RFID communication, power harvesting, a power supply module, and an SPI Master circuit connected to a microcontroller for use in a Tire Pressure Monitoring System. The ANDY100 is used for energy harvesting and wireless communication while tested in car tires, allowing the MS5803-14BA temperature and pressure sensor to communicate over a meter and a half using a 2W ERP setup. The work presented by Vena et al. [38] demonstrates an entirely passive long-range UHF RFID tag for monitoring the tilt and temperature of fragile objects during transportation. The RFID tag by Vena et al. combines the Farsens Rocky100 IC connected directly to a 3-axis accelerometer ADXL362 without using a microcontroller. The RFID tag can detect movement and sense temperature while harvesting UHF RF power at a distance of 1m.

2.2.4 Powercast

The Powercast Sensor Tags allow RFID technology to monitor environmental factors using temperature, humidity, and light sensors [39]. The PCT100 sensor tag utilizes the Powercast Powerharvester® Chipset, eliminating the need for batteries. The sensing tag converts RF energy from an RFID reader, i.e., TX91501B, or for collecting sensor data. Powercast® offers two main types of sensor tags: the PCT100 and the PCT200. The difference between the PCT100 and the PCT200 is that the first one offers completely battery-free wireless sensing. In contrast, the second one has a rechargeable battery with a life of up to one month, which is ideal for data-logging applications. The TX91501B and TX91503 are 915 MHz Powercaster® reader transmitters with 1 and 3 watts EIRP. This type of reader supplies power and data to devices with a 60° width, 60° height vertical polarization beam pattern, and Amplitude Shift Keying (ASK) modulation [40]. The Powercast sensors and readers are commercially available, and the company seeks to expand the market to devices powered and wirelessly charged using directed RF waves.

2.2.5 Wiliot

Wiliot is a company fabricating tiny battery-free tags that harvest energy from ambient radio waves. Wiliot Pixels are small, cost-effective RFID tags that harvest energy from ambient radio waves, enabling battery-free Bluetooth communication over 10 meters. They incorporate an ARM Cortex M0+ 32-bit operating at 1 MHz, 128-bit AES encryption security features, at a low cost as low as 10 cents.They integrate with Bluetooth-enabled devices, such as smartphones and access points, and offer sensing functionalities like temperature, humidity, and location. [41].

2.2.6 Confidex

Confidex tags are Industrial-grade RFID and NFC. Among their multiple application, they enable Industrial IoT. A wireless industrial equipment monitoring solution developed together with Turkish R&D company Environics Applied Sciences Inc. offers a vibration analysis solution known as Able System® that identifies the conditions of machinery and the components within those machines in industrial environments. It uses the Confidex ruggedized UHF RFID tag "Ironside Micro" in UHF and NFC versions [42].

2.2.7 STEVAL-PROTEUS1: Wireless Sensor with Battery

The STEVAL-PROTEUS1 [43] is a robust industrial sensor evaluation kit designed by STMicroelectronics for temperature and vibration monitoring in industrial applications. It is not an RFID-based sensor but is included here as a standard to look at and compare our work. Includes a 2.4 GHz RF supporting Bluetooth Low Energy 5, 802.15.4, Zigbee 3.0, and Thread for monitoring, dual-core 32-bit Arm Cortex-M4 MCU 64 MHz powered by a 3.7 V, 480 mAh LiPo battery. The STEVAL-PROTEUS1 includes sensors like the IIS3DWB accelerometer with high bandwidth, the IIS2DLPC ultra-low power sensor, the ISM330DHCX inertial module (accelerometer and gyroscope) with MLC and STTS22H temperature sensor. The platform includes the STSAFE-A110, whith data security, and a phone app, ST-BLE Mesh, which offers real-time measurements. Although this module relies on a LiPo battery, it includes all the desired sensing functions for preventive maintenance and Industry 4.0 applications we desire for state-of-the-art CRFID design.

2.3 CRFID Comparison

Table 2.2 shows a comparison between CRFID systems, their computation, sensing capabilities, and limitations. Among the works mentioned, WISP was one of the first to implement computation based on RF power, adding a unique dimension to its use cases as a flexible, open-source platform.

Device	RF Frequency	Computing	Sensor	Working Distance	Reference
WISP	UHF RF (915 MHz) Solar	MSP430	Motion, strain, acceleration	3-4 m	[28–31]
FARSENS	UHF RF (915 MHz)	ROCKY100, ANDY100 IC	Temperature, pressure	Few meters	[36–38]
POWERCAST	UHF RF (915 MHz)	Powercast Power Harvester Chipset	Power Harvester	Few meters	[39, 40]
Wiliot	Ambient RF (Wi-Fi, cellular, Bluetooth)	ARM Cortex M0+	Temperature, humidity, proximity	10 m	[41]
Confidex	UHF RF (915 MHz)	NXP UCODE 7xm	Temperature	7 m	[42]
VCRFID ***this work***	**UHF RF (915 MHz)**	**EM4325 virtualized interface**	**Temperature, vibration, SPI COTS**	**2-3 m**	[44]

Table 2.2: Comparison of CRFID works and state-of-the art

From the data presented in the table, Wiliot emerges as a strong alternative for applications requiring longer working distances and robust computing capabilities, thanks to its ARM Cortex processor and ability to harness energy with a -35 dBm reported sensitivity from Bluetooth and various ambient RF sources. On the other hand, Confidex RFID tags offer a balanced mix of computing power and sensor support intended for use in industrial high-temperature settings.

In comparison, the VCRFID range is less than that of Wiliot or Confidex, but a higher-sensitive RF harvester like the one presented in Chapter 6 with a -31.4 dBm sensitivity could contribute

to extending the VCRFID range beyond the initially reported distance. Moreover, the VCRFID work through the virtualized SPI interface facilitates the integration of Commercial Off-The-Shelf (COTS) sensors. This innovative method not only allows for the seamless incorporation of a wide variety of sensors into the RFID system but also introduces a high degree of reconfigurability and adaptability beneficial in dynamic environments across numerous applications that other works like Wiliot and Confidex lack.

Chapter 3

VCRFID: A Virtualized Controller for CRFID

3.1 Motivation: Wireless Sensing on Limited RF Power

Ensuring high efficiency in end-to-end energy harvesting is crucial for devices that require intricate mechanisms for RF communication and computation. This necessity stems from the requirement for a microcontroller to oversee the operation of embedded sensors. The added elements that regulate each of the devices' mechanisms not only increase the power requirements but also increase the complexity and cost of the device.

CRFID devices combine the computational power normally offered by microcontrollers with augmented RFID capabilities such as telemetry, providing an all-in-one solution for various IoT applications [45–48]. With the help of computational techniques, CRFID systems can offer advanced

functionality, such as data analysis [49], edge computing [50], and advanced decision-making [51] at a low cost. CRFID technology is an ideal passive solution for autonomous tasks like monitoring applications in remote environments where RF power is limited.

3.1.1 Microcontrollers on RFID Tags

In applications that involve sensors, typically, a controller device, as shown in Fig. 3.1, is set to handle the operation, stream data, and talk to peripherals through interfaces such as SPI or I^2C. To operate the microcontroller, in addition to requiring added functionality blocks such as controllers, and other peripherals, the power management block is a critical part of the design. However, This design complexity leads to increased demands for processing capability and energy consumption on the microcontroller-based devices [48, 52].

Conventionally, batteries have been the primary source of energy to meet these requirements. Still, the major challenges associated with battery-powered IoT devices are that their power is limited and tied to the battery charge, resulting in a finite lifespan and environmental impact.

To address this limitation, RF power harvesting is employed in various wireless sensing platforms [53, 54]. The use of RF energy harvesting enhances device longevity and decreases environmental consequences, promoting sustainable energy use in IoT deployments. It also emphasizes the importance of innovative power management in supporting sensor-based devices.

CRFID tags offer several advantages as IoT devices, but there are some important factors to consider:

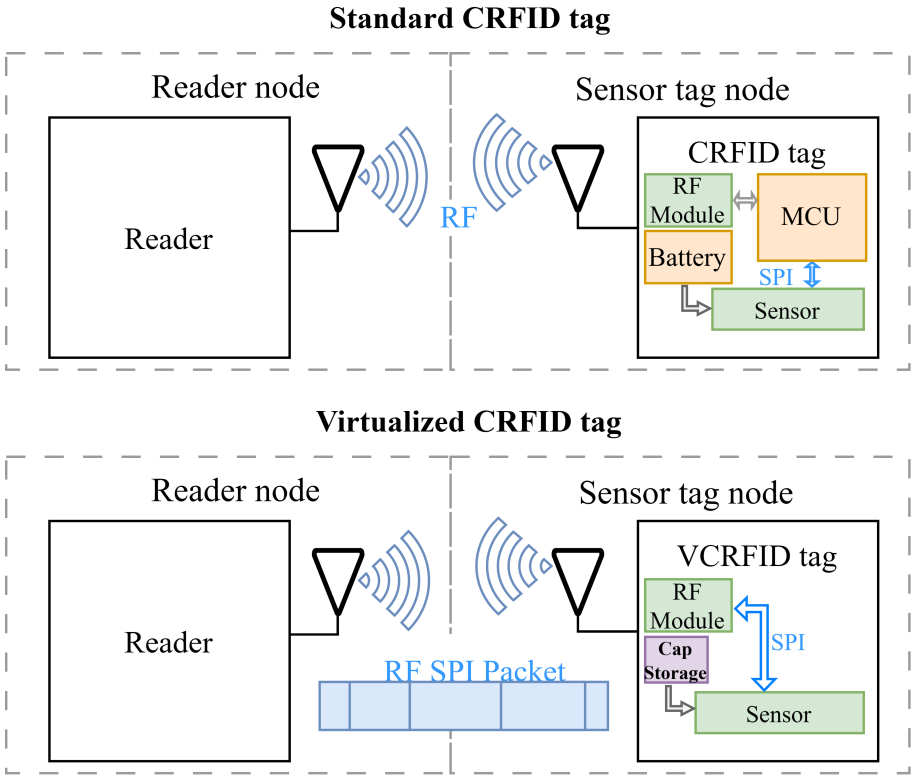

Figure 3.1: Comparison of system architecture and key components between a standard Computational RFID system (CRFID) and Virtualized Computational RFID (VCRFID)

- Integrating sensors on an RFID tag usually requires the use of a microcontroller or peripheral controller.

- A lack of flexibility since reconfigurability of the node, in software or hardware, is not possible without physical access and direct modification to the CRFID tag.

- On battery-depending devices, the overall cost, and maintenance, including charging or replacing the battery, is larger compared to that of RF harvesting devices.

- Balancing low power requirements and high performance is challenging in sensing CRFID tags due to the microcontroller's high power consumption.

3.1.2 Balancing Power Consumption

Various techniques can contribute to reducing power consumption and making the devices more energy-efficient, one of which is duty cycling, periodically turning on and off the devices [55]. Another is dynamic voltage scaling, a technique to adjust to the consumed power as is required [56]. Notably, standby mode operation, marked by static leakage power, contributes to substantial energy loss, exacerbating concerns related to short battery lifespans. Finally, another way to extend the device energy lifespan is designing ultra-low power devices [57]. Ultimately, all previously mentioned energy-saving techniques exist at the expense of trade-offs. The proposed Virtualized Computational RFID (VCRFID) system tag design maximizes harvested RF and decreases the number of elements actively consuming power through the introduction of the concept of a virtualized controller for CRFID.

3.2 Virtualized Controller as Solution

We introduce an approach that focuses on eliminating the high power consumption of microcontrollers and addresses some of the issues associated with CRFIDs as IoT devices. This new system architecture achieves this goal by offering two key features: (1) wireless control of sensors and (2) sensory data computation.

We propose shifting control and computational functions from the tag to the reader. The reader performs the more computationally intensive operations, thus saving energy on the tag and reducing

the tag's power consumption. By eliminating the microcontroller, energy-demanding operations shift to the reader via RF commands. We achieved the virtualization of the microcontroller's functions using custom SPI instructions sent and received by the reader over RF. In summary, the VCRFID design achieves the following:

1. Virtualization of serial peripheral interface bus and controller through custom SPI commands over RF. Offloading power-intensive functions from the tag to the reader eliminates the need for a microcontroller on the tag to control the sensors.

2. A simplified ultra-low energy device design performs more efficient energy management for self-power and to power additional sensors or devices on the tag without the need for batteries.

3. Wireless control and reconfigurability, allowing new functions to be implemented with a set of SPI instructions sent from the virtualized controller via RF. This is so that the configuration and operation of the system are modified as needed on the fly, without required physical access to the tag, and quickly adapt the system to changing needs or conditions.

3.2.1 Design for Wireless Data, Power, and Sensing

As shown in Fig. 3.2, we design a sensing system consisting of a tag and a reader node as the main elements. The VCRFID system tag is designed with a receiving antenna, a sensing module, and an RF IC for managing RF communications and long-distance energy harvesting from the transmitted reader signal.

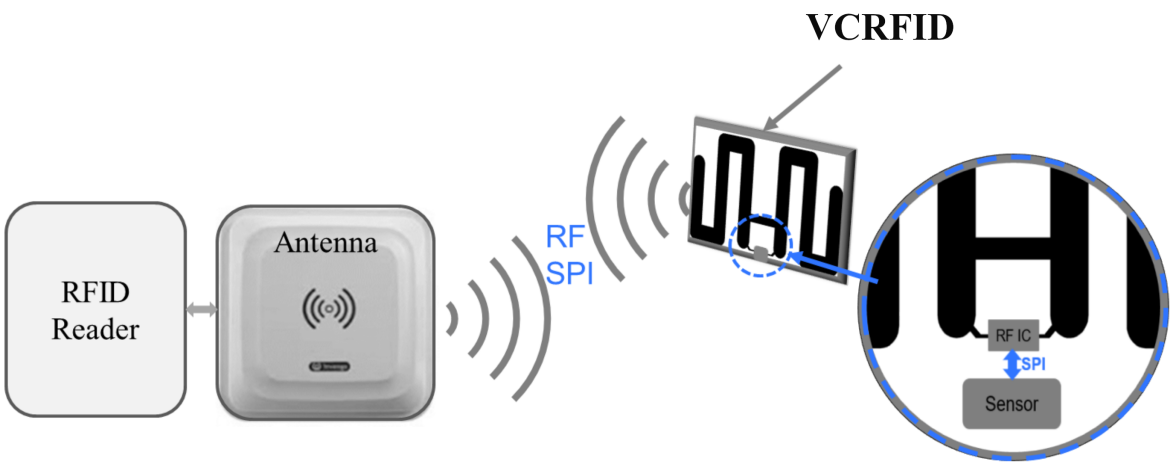

Figure 3.2: VCRFID system overview. The system comprises a reader and a tag with an RF chip and embedded sensor. The sensor data is transmitted wirelessly in packets via the virtualized controller interface from the sensor to the reader through the RF IC.

A controller device handles the operation of peripherals, particularly communication between integrated circuits, for example, the sensor and the RF front-end IC, and performs computational tasks. In our design, the VCRFID system employs virtualized instructions to control data transmission and sensor operation and does not require a microcontroller to be built on the tag. The operation is completed using RF instructions transmitted between the sensor and the reader node. These instructions handled by the reader are SPI signals over RF packets, which we can refer to as SPI-over-RAIN. This eliminates the need for a microcontroller on the VCRFID system tag to manage the sensing functions, as well as removing the need for a battery to provide additional power to the microcontroller.

The power required to operate the RFID tag is transmitted by the reader, which emits an RF signal that is received by the antenna on the tag. Once the tag receives this signal, the energy harvesting

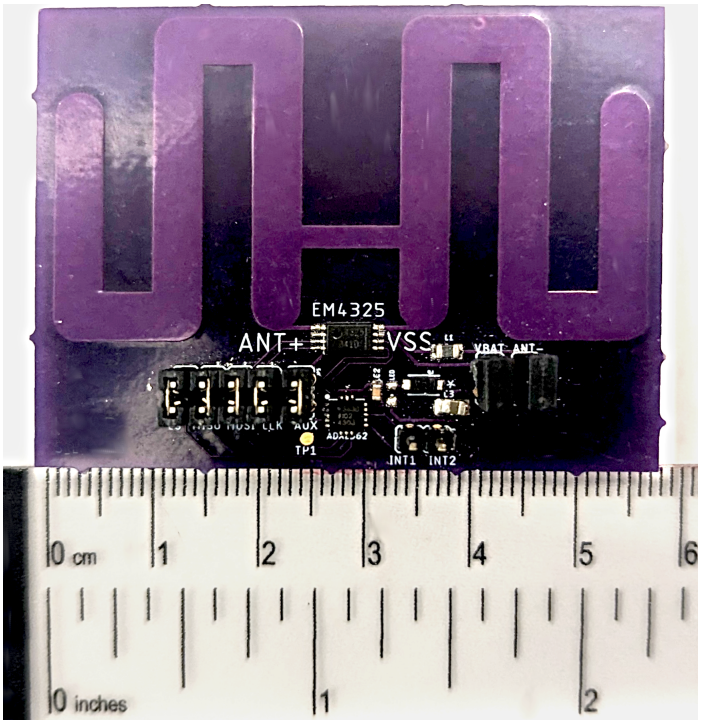

Figure 3.3: VCRFID system tag prototype with meandered dipole antenna, RF IC (EM4325), and sensing module built on an FR4 substrate.

process in the tag RF IC converts the RF energy into usable electrical energy, which is then used to power the components embedded in the tag. The custom RF commands are transmitted between the reader and the tag's RF IC, which is directly connected to the sensor.

To experimentally validate the main ideas related to the virtualization of the VCRFID functionality, we fabricated a tag prototype on a 4.5 cm x 5.7 cm FR4 board with a receiving meandering dipole antenna and an RF module composed of an EM4325 IC [58] and sensor module with a 3-axis ADXL362 accelerometer [59], see Fig. 3.3. Then, the ST25RU3993-HPEV board from ST Microelectronics was set as the reader node for the VCRFID system. Operation of the tag and all the RF communication is carried out in the UHF band at 915 MHz. Custom SPI commands are sent from the virtualized controller at the reader over RF for reading, writing, and accessing the

sensor data in real-time. Fig. 3.4 shows the communication exchange between the reader and the VCRFID system tag. Initially, the reader establishes communication with the tag and receives the backscattered tag ID or EPC code signal. After that, the reader sends the custom RF command SendSPI, containing an SPI packet. In the case of a "read sensor" command, the SPI packet includes the SPI read command size, the response's byte count, the SPI SCLK setting, the SPI delay time, the SPI delay time between bytes, and the sensor SPI command.

3.3 VCRFID Power Evaluation

We can estimate the energy consumed by the EM4325 RF IC during a read of the tag-ID from the measured voltage drop. Each read operation consumes an estimated 400 mV from the capacitor charge. During the duty cycle, after the read operation is completed, the charge is restored with the energy harvested by the EM4325. We can calculate the energy consumed per sensing operation from (3.1), where $V_{Max} = 2.5\ V$, $V_{Min} = 2.1\ V$, and for a chosen $C = 44\mu F$. We can estimate E_{load} = 52 μJ.

$$E_{load} = \frac{1}{2}\, C(V_{Max}^2 - V_{Min}^2) \tag{3.1}$$

The energy feasibility condition for a particular sensor can be expressed as:

$$V_{dd}(I_S + I_W)T \geq \frac{1}{2}C(V_{\text{rec}}^2 - V_{dd}^2) \tag{3.2}$$

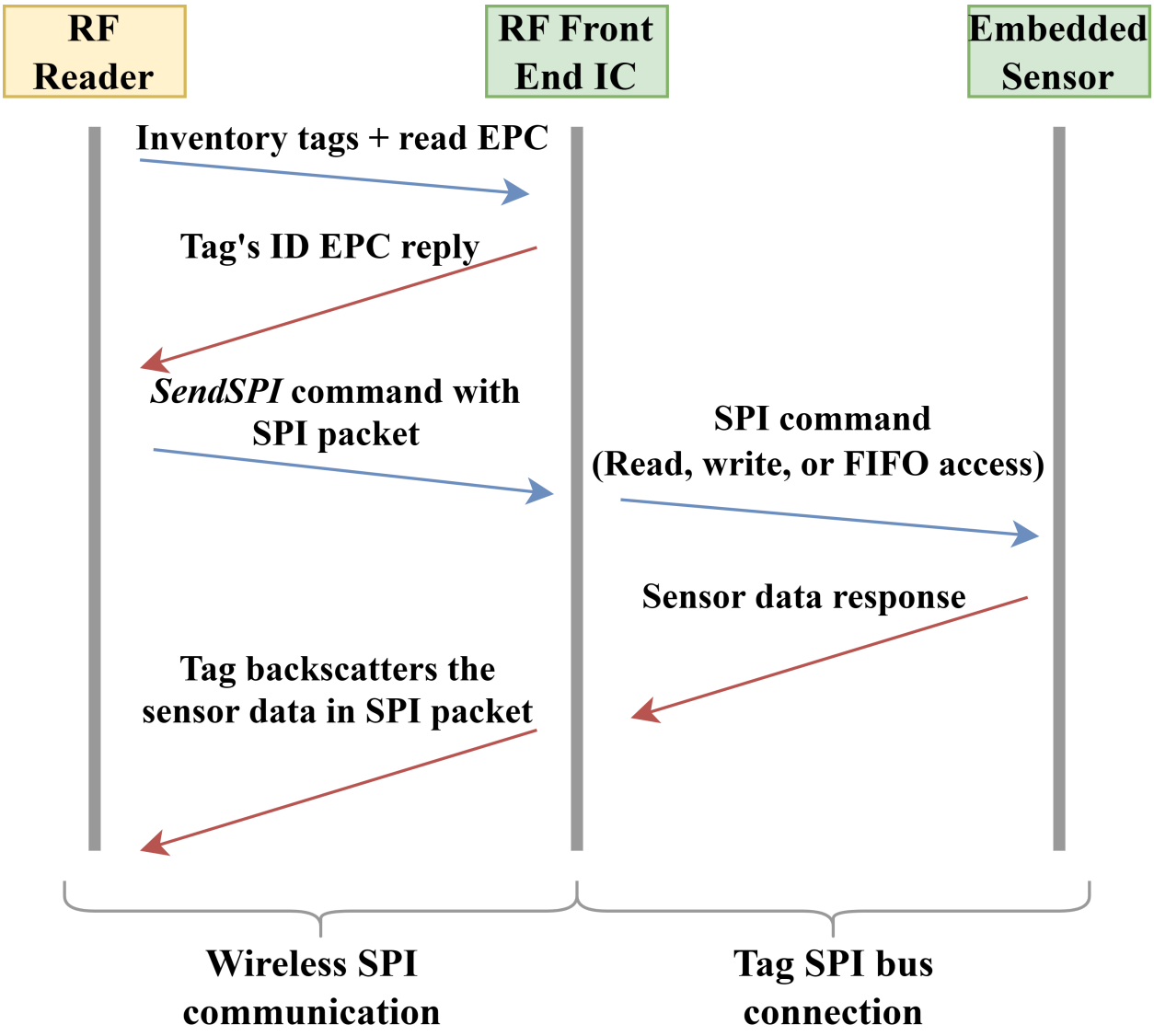

Figure 3.4: SPI communication exchange between the RF reader and the VCRFID system tag

Where the energy required to read the sensor must not exceed the usable stored energy. This expression can be used to calculate the capacitor size and voltage headroom required.

The current consumption for the sensor and RFID tag are I_S and I_W, respectively; C is the capacitance of the storage capacitor, and T is the total time of active operation. The rectified voltage is V_{rec} and V_{dd} is the required operating voltage. Assuming that the sensor has the same voltage

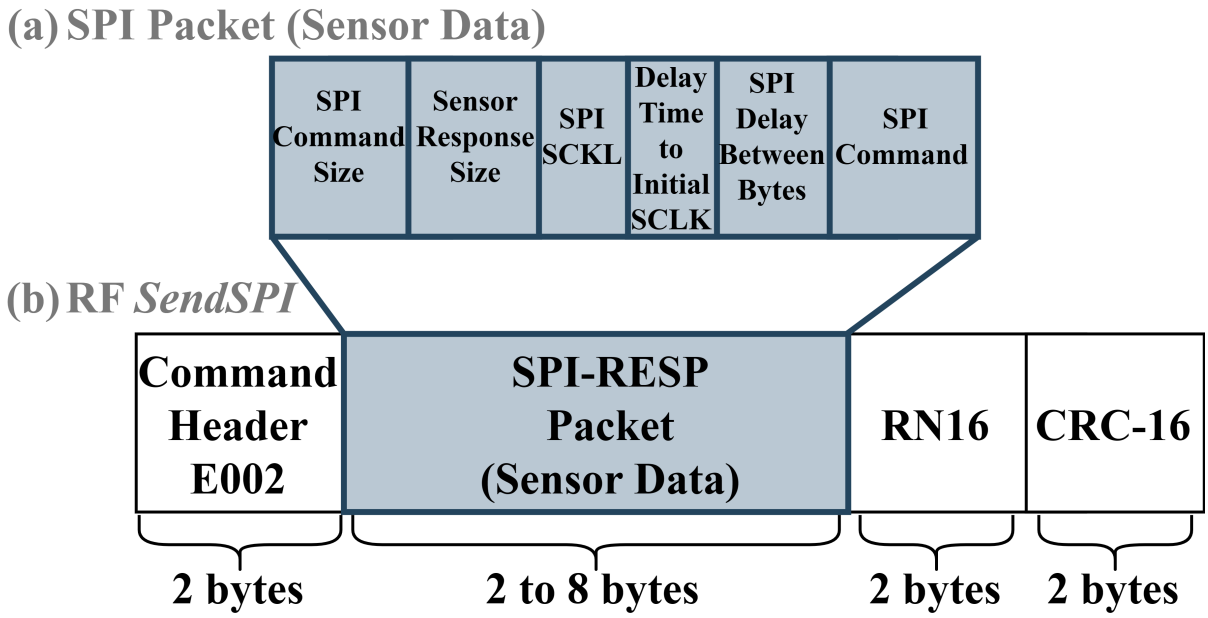

Figure 3.5: Data packet structure of the custom RF SendSPI command transmitted between reader and tag.

supply as the RF IC, $V_{dd} = 2V$. The left-hand side of inequality represents the energy consumed by the sensor and the tag during one operation. The right-hand side represents usable stored energy above V_{dd}, the minimum operating voltage of the tag. The equation makes it clear that the limiting factor when selecting sensors is not only the current consumption (which determines power) but also the total required execution time of the sensor and RFID tag (energy rather than power).

Given a transmitted power fixed at 30 dBm for a frequency of 915 MHz, with the transmit antenna gain at 6 dBi, and the receive antenna gain at 2 dBi, we can calculate the received power at various distances using the Friis transmission equation. The effective isotropic radiated power (EIRP) is thus 36 dBm, adhering to the FCC limit for a UHF RFID reader.

The wavelength λ is calculated as follows:

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8 \text{ m/s}}{915 \times 10^6 \text{ Hz}} \approx 0.328 \text{ meters}$$

Using the Friis transmission equation in dB form:

$$P_R(dBm) = P_T(dBm) + G_T(dBi) + G_R(dBi) - 20 \log_{10}\left(\frac{4\pi r}{\lambda}\right)$$

where P_R is the received power in dBm, and r is the range in meters.

We can compare the calculated power consumption of the VCRFID system tag to other battery-less RF harvesting CRFID sensing systems. The tag's total consumed power will vary depending on the load that's embedded in it. The bar chart in Fig. 3.6 shows that the computational component has the most significant power consumption. The UHF-RFID systems [52] based on the EM4325 RF IC and the WISP tag [48] require microcontrollers to handle the sensor's control and computation. The VCRFID system tag's power consumption comes mainly from the RF IC responsible for RF communication and the attached sensor. Moreover, the tag's power consumption is considerably lower, indicating a 97% reduction in energy consumption compared to other energy-harvesting RFID tags that incorporate microcontrollers for sensor operation in their circuit.

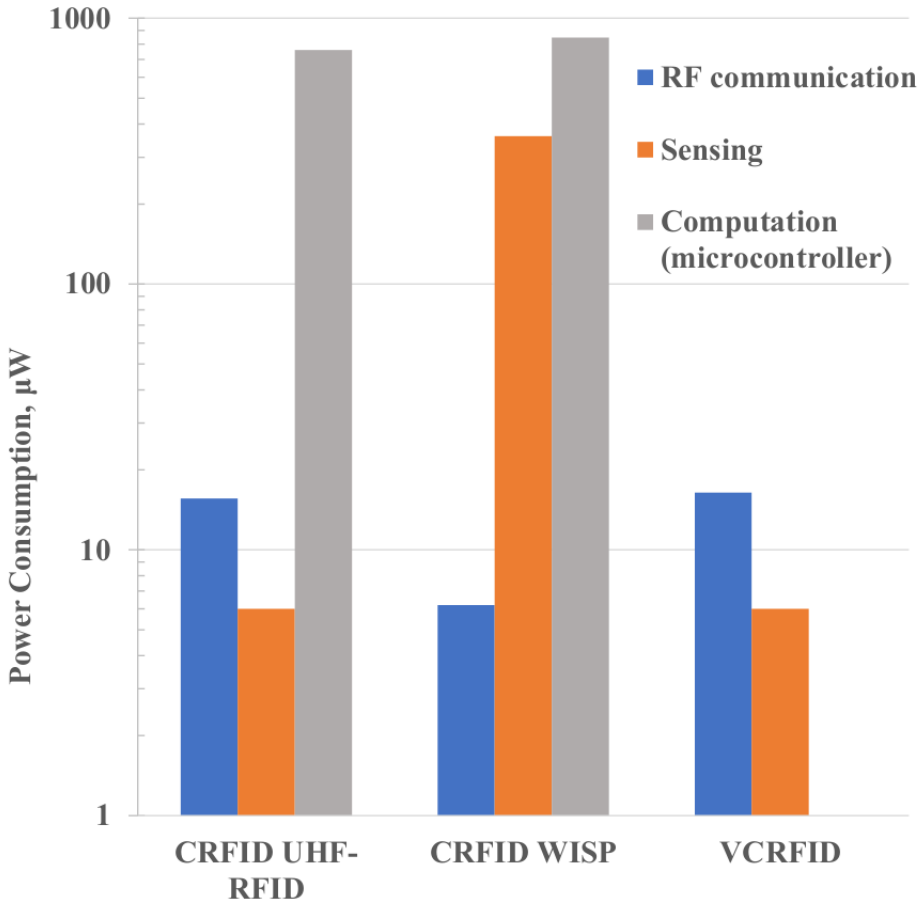

Figure 3.6: Power consumption comparison and breakdown of the consumption per category. We can see that most of the consumption on the CRFID WISP and tag based on EM4325 with embedded microcontrollers for sensing applications comes from computational operations, while on VCRFID, it is from RF communication.

3.4 Vibration Detection

Figure 3.7 shows vibration data collected wirelessly using the ADXL362 sensor in the VCRFID system tag. The system demonstrated successful SPI communication and sensing with the tags at distances of up to 3 meters. However, to ensure packet integrity at the higher frequency required for the vibration test, we positioned the target device 50 cm away from the reader. Using the tag mounted on the device under test, we collect 3-axis acceleration data in real-time, representing the

device's vibration and displacement.

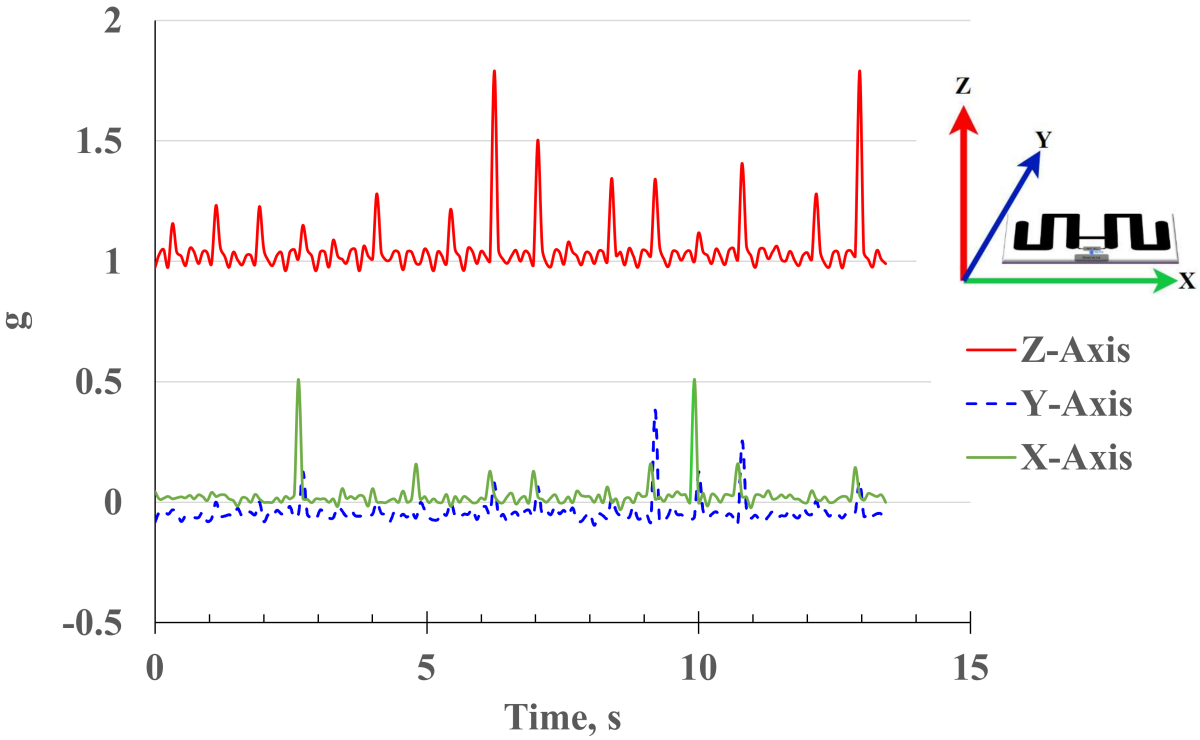

Figure 3.7: Plot with vibration data of the 3-axis ADXL362 sensor on the VCRFID system tag.

A periodic signal observed in the vibration plot shows a harmonic repeating pattern. The vibration pattern is particularly visible on the Z-axis, representing a movement perpendicular to the surface. The acquired signal can be further analyzed to identify the type of faults in the vibrating equipment based on the patterns observed. With the vibration data acquired through the tag, it's possible to remotely monitor equipment such as motors, fans, and machines. Because of their simplicity, reliability, and long-life design, VCRFID system tags are ideal for this type of application. These features of the VCRFID device are valuable for numerous applications in remote locations, including anomaly detection, pattern recognition, and predictive maintenance [60, 61].

Chapter 4

Wireless IoT Sensor Networks With Edge-Powered VCRFID Devices

4.1 Edge Solutions to the Data Deluge

The emergence of trillions of diverse, interconnected sensing devices further accentuates the complexity of wireless network ecosystems. A significant concern arising from the expansion of IoT sensing devices is the overwhelming amount of data, the data deluge [14]. We may reach a point where our ability to generate analog data surpasses our capacity to efficiently utilize it, potentially impeding the retrieval of valuable information when required. In devices connected to the cloud, we encounter problems such as limited data bandwidth, delays in data transfer to the cloud, higher energy use due to large data handling, and security concerns [62, 63]. In this evolving landscape,

edge devices have the advantage of being near the information source. However, a drawback associated with edge-based devices is their constraints in computational resources, memory capacity, and power budget [64, 65]. In addition, a notable challenge is achieving the perfect equilibrium among ease of implementation, affordability, and scalability, all key for IoT connectivity solutions.

4.2 State of the Art

Previous research has explored the utilization of RFID tags for various sensing applications, specifically employing the Gen2 EM4325 IC developed by EM Microelectronic. The EM4325 is a versatile RFID IC that operates as both a passive and battery-assisted passive RFID IC. The EM4325's unique capability ensures its robust performance across various applications in an efficient and adaptable mode for RFID technology solutions. The adoption of the VCRFID system facilitates the creation of advanced smart sensing platforms, enhancing data collection and enabling operation in varied and demanding conditions, as demonstrated in the next section.

4.2.1 Related Works

In the study conducted by [32], RFID tags incorporating the EM4325 IC were used for epidermal body temperature measurements. Likewise, in the works by [33–35], this RF IC is used for temperature measurements, with each study creating new designs for the RFID tag antenna tailored to their specific application. The work by [66] introduced an ultra-low power virtualized computational RFID tag system that leverages a virtualized SPI interface over RF to enhance sensing

capabilities in EM4325-based tags. Among others, all these works are a brief highlight of the widespread adoption of RFID tags and collectively underscore the widespread adoption of RFID enabled sensors.

For machine learning applications that include RFID tags as sensors, the authors in [67] developed a Bayesian Regularization classifier ML model that performs structural health monitoring by detecting cracks on conveyor belts. The authors in [68] developed a classification algorithm based on Support Vector Machines to identify ripe fruits using RFID sensing tags that measure chemicals released by the fruit. However, to our best knowledge, no previous research combines battery-less VCRFID sensing and temperature anomaly detection using LSTM at the edge.

4.3 Edge-Powered WSN Based on VCRFIDs

We analyze the use of ultra-low power VCRFID tags for Wireless Sensor Networks (WSN). We aspire to facilitate seamless data exchange and device connectivity without relying on physical cables or batteries. We find this solution ideal for scenarios where strict limitations on device size, weight, and access to power are heavily restricted, such as aircraft, deployed vehicles, or remote location monitoring.

In this work, we implement an edge-powered RFID-based IoT sensor platform to monitor sensor data, such as indoor temperature conditions, and access real-time temperature data.

The VCRFID IoT platform provides programmable functionalities and supports a wide array of

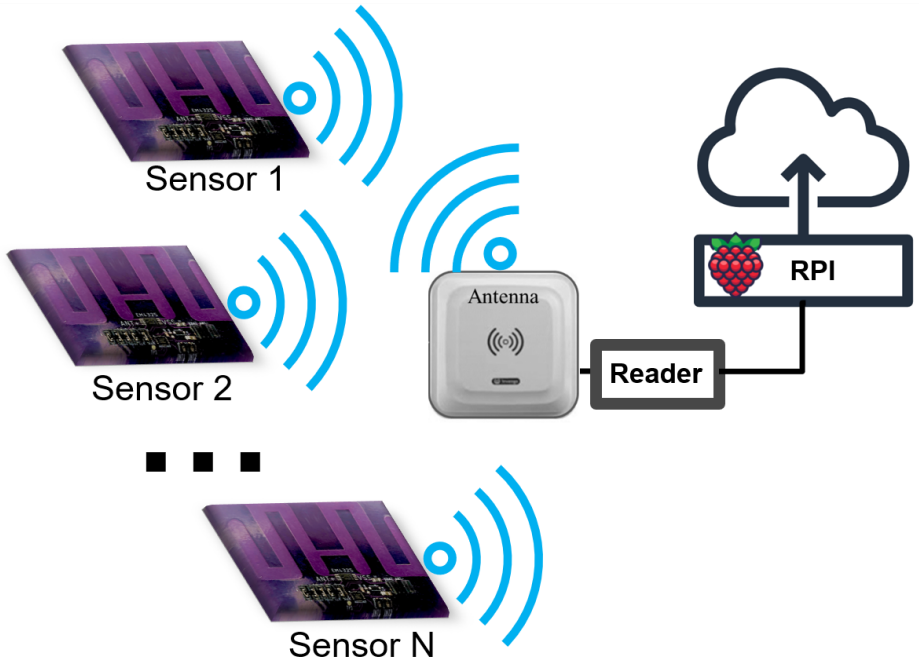

Figure 4.1: Edge-powered VCRFID IoT wireless sensor network (WSN) system overview. The VCRFID-WSN system comprises multiple RFID tags that communicate with and are powered by an RFID reader, which serves as the immediate data collection and processing point. The RFID reader is connected to a host computer, which functions as an edge computing node. This host computer is equipped with advanced processing capabilities, such as ML methods, that allow for immediate data analysis and decision-making at the local level before any data is sent to the cloud.

sensors, including temperature sensors, accelerometers, and other types of Commercial Off-The-Shelf (COTS) SPI-interconnected sensors. The VCRFID-based sensor network is comprised of three main components, as shown in the diagram in Fig. 4.1. Central to its architecture is a reader connected to an antenna, set for optimal RF data reception and transmission at a frequency of 915 MHz. The reader is connected to a Raspberry Pi that manages the hardware firmware and executes the program to log the sensor data. The sensor network comprises an array of battery-less and wireless IoT sensors, with each sensor embedded within VCRFID tags powered by the transmitted RF signals. We use ultra-low-power VCRFID system tags, first introduced in [66], for the WSN. The VCRFID system tags offload computationally intensive operations to the reader

while harnessing their energy from the RF reader. These tags form the core framework for the network's sensing functionalities. If the number of sensors needs to be increased, no additional operation is required for the new sensing device to be added to the network. Ready to deploy, all that is required is to bring the RFID-based IoT sensing device within range of a reader.

4.3.1 RF Power at the Edge

The VCRFID-based IoT platform's RF harvesting element can mitigate the challenges of power constraints and a limited battery lifetime. The passive VCRFID sensing devices enable self-powered and sustainable battery-less sensor operation. The RFID reader antenna radiates electromagnetic energy that is harvested by the tags and used to power the tag's IC.

Fig. 4.1 shows a diagram representation of the proposed VCRFID system, consisting of interconnected battery-less and wireless sensing tags in a small form factor that performs the function of a flexible IoT sensing platform. The reader, linked to the antenna, serves as the hub, responsible for sending and receiving RF signals to and from the VCRFID system tags. RF is used for communication and power. The Raspberry Pi serves as an intermediary host between the reader and higher-level systems. These three components establish the foundation of the proposed wireless sensing platform and data acquisition.

4.4 WSN Temperature Application

We demonstrate the integration of VCRFID sensor tags as a cost-effective tool for sensing and collecting temperature data. For this, we analyzed the RFID tag's performance in sensing temperature variation. We employed the tag's RF IC EM4325 (EM Microelectronic) for the temperature measurements. The RF IC temperature sensor specifications indicate a typical accuracy of $\pm 1.0°$C when operating in the range of $-40°$C to $+60°$C [58].

The sensor data was transmitted to the reader (ST Microelectronic ST25RU3993-HPEV) at the US 915 MHz operating frequency. The battery-less, ultra-low power VCRFID sensing devices' design allows for configuration flexibility, which means the sensing devices can be reconfigured to support various types of SPI-controlled sensors using a virtualized SPI interface as described in [66]. Similar to the temperature sensor example in this paper, the system can be set to obtain humidity, vibration, acceleration, and position if desired sensor is connected via SPI to the tag. The use of the VCRFID system sensing tags enables temperature monitoring applications in locations with restricted access and power constraints where physical access is difficult. In the described VCRFID-based edge computing system, processing and data storage occur within the reader and Raspberry Pi host device near the data source. This approach allows for data pre-processing, decreasing the amount of data intended for transfer to the cloud. Consequently, it efficiently mitigates the expenses associated with data transmission and accumulation within the cloud infrastructure.

4.4.1 Temperature Data Analysis

The primary objective of this section is to analyze the temperature sensing capabilities of the VCRFID system tags. We evaluated the potential of these tags to gather and relay temperature data at regular intervals. For the experiment, a sensing tag was exposed to sudden temperature fluctuations, alternating between periods of heating and cooling. The temperature readings obtained from the VCRFID system tag were collected and compared against the temperature measurements concurrently recorded using a thermocouple (Elitech Tlog-100). This process allowed us to gauge the accuracy and reliability of the sensing tags in capturing temperature data under varying conditions.

Fig. 4.2 shows the temperature data collected and monitored using a single VCRFID IoT system tag of the sensor network every 30 s. The sensing tag was exposed to heat and cold. Temperature data were collected every T = 30 s using the tag's EM4325 IC and compared to the temperature recorded with a thermocouple.

To find the accuracy of the tag measurements, we compare the data points from both the tag and the thermocouple for the same time intervals. To calculate the difference between the two readings at each time interval, then average these differences to get the measurement mean error. This mean error can then be expressed as a percentage of the total range of temperatures recorded. Although some variation is observed between the thermocouple and VCRFID data collected, particularly at sudden rises and falls in temperature, the measurement's accuracy between both sensing elements

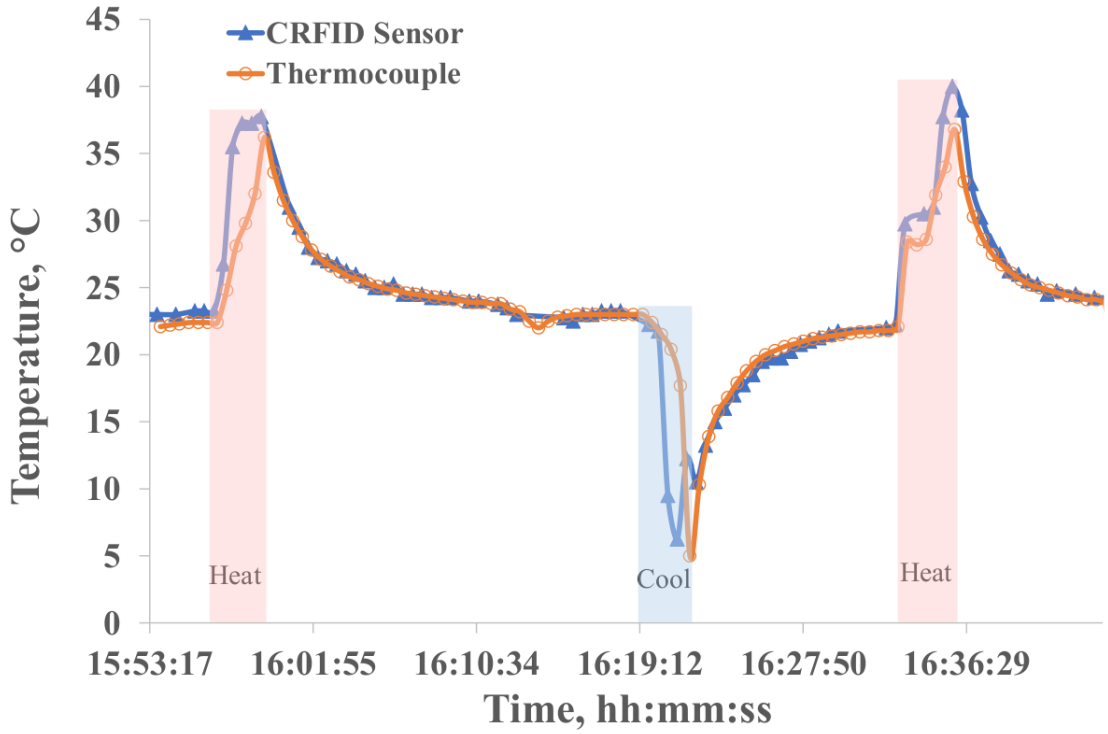

Figure 4.2: Temperature data collection and monitoring example using a VCRFID system sensing tag. The VCRFID system sensing tag was exposed to heat and cold. Temperature data were collected every T = 30 s using the tag's EM4325 IC and compared to the temperatures recorded with a thermocouple.

is consistent. This suggests that the WSN, with its VCRFID system sensing tags used for real-time temperature monitoring in various applications, can reliably replicate traditional sensing methods while offering the advantages of wireless connectivity and remote monitoring capabilities without the battery limitation.

4.5 Temperature Anomaly Detection

In this section, we analyze the temperature data acquired from a VCRFID WSN. The system uses an LSTM autoencoder model for anomaly detection in temperature variations. We configured the Raspberry Pi to oversee the anomaly detection model, manage the reader, and aggregate the sensor data. We run an optimized lightweight LSTM autoencoder model with the help of TensorFlow as the backend on the Raspberry Pi.

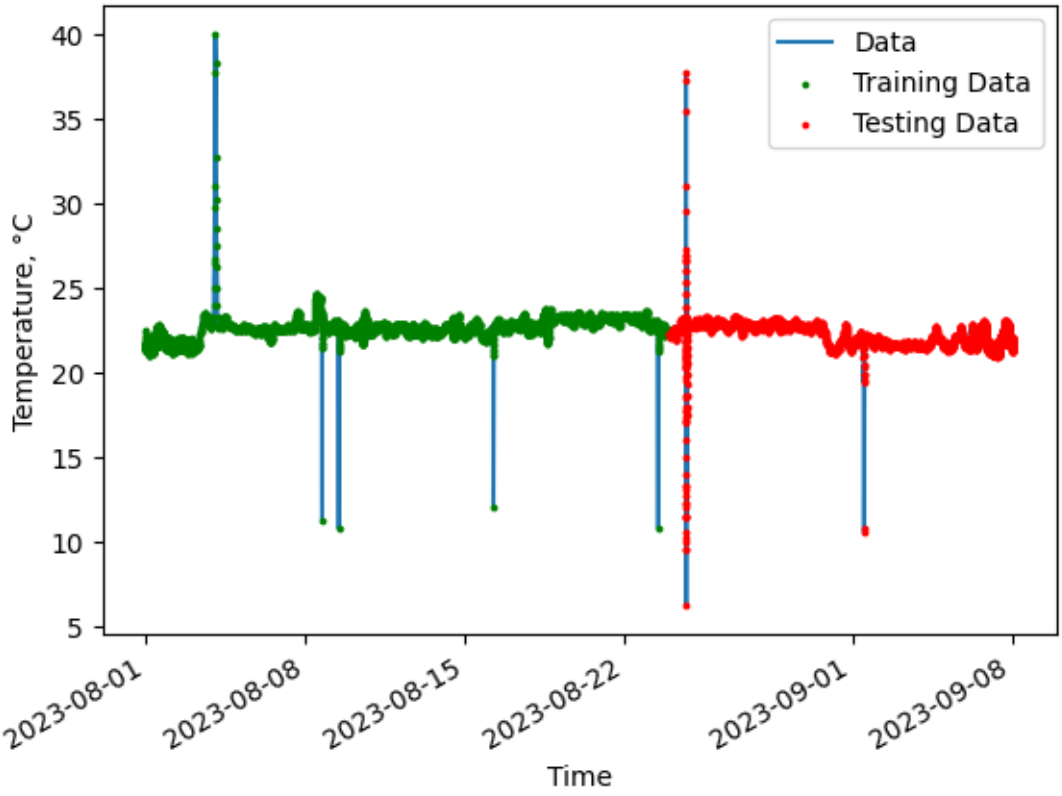

Figure 4.3: Temperature dataset collected by the VCRFID sensing tags. A segment of temperature data, shown in green, is used for training the model, and the rest, shown in red, for testing.

The data used in this work, shown in Fig 4.3, was collected for over a month from a WSN consisting

of three tags in the VCRFID system that measure the room temperature every half hour using an EM4325 RF IC and transmit that data at 915 MHz via RF to the reader. The resulting plots show the capabilities of VCRFID system tags as IoT devices in a WSN and serve as an example of an anomaly detection system powered by the edge.

As shown in Fig. 4.3, the sensor data was partitioned into subsets: 70% allocated for training and the remaining 20% part designated for testing. The model training is then validated with 10% of the data allocated for validation purposes.

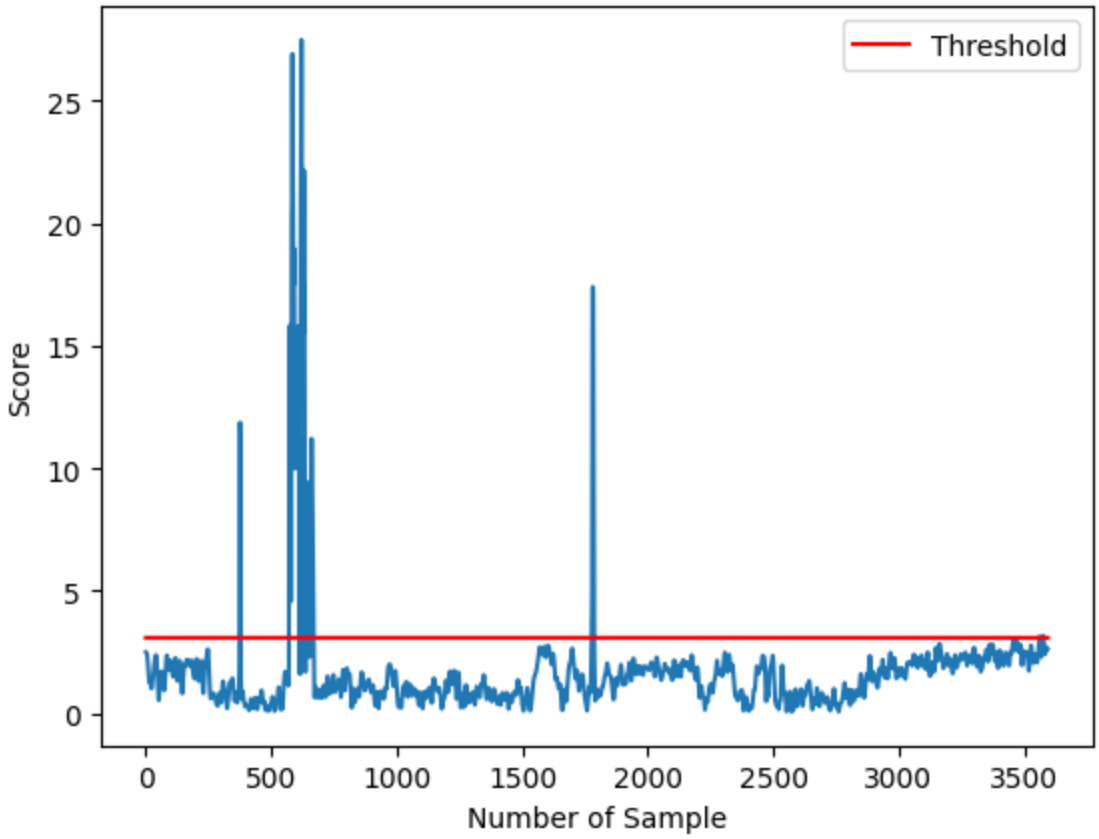

Figure 4.4: Plot of the error score associated with the samples. A low reconstruction error indicates that the input data is similar to what the autoencoder has seen during training. A high reconstruction error suggests that the input data significantly deviates and represents an anomaly.

As defined by Chandola et al., an anomaly is a pattern in data that does not conform to a definition of normal behavior [69]. The primary output from the LSTM autoencoder model is the reconstruction error observed in Fig 4.4, which measures how well the model can reconstruct the input data. Considering the standard deviation σ of the temperature data's normal distribution, we established the threshold value and validated the results through event observation. Data points exceeding 2σ, for a threshold ratio over 0.95% of the samples, are identified as outliers. Reconstruction errors with high values indicate anomalies, while values within the threshold limits are regarded as normal. We determine which data points are considered anomalies and which are considered normal based on the reconstruction scores and threshold.

4.5.1 Temperature Anomalies Detected

Data points indicating anomalies provide insights into patterns of temperature variation and the predictive capability of the LSTM autoencoder model. The detected anomaly data points, as illustrated in Figure 4.5, represent the temperature anomalies detected. The temperature anomalies detected, highlighted in red, are plotted over the temperature data gathered by the sensors shown in blue. To understand the performance of the LSTM autoencoder model during training, we analyze the training loss and validation loss, which suggests that the model will respond well to new data that the model has not seen during training. A larger dataset would likely enhance the model's performance.

The anomaly detection was implemented using an LSTM autoencoder and integrated at the edge.

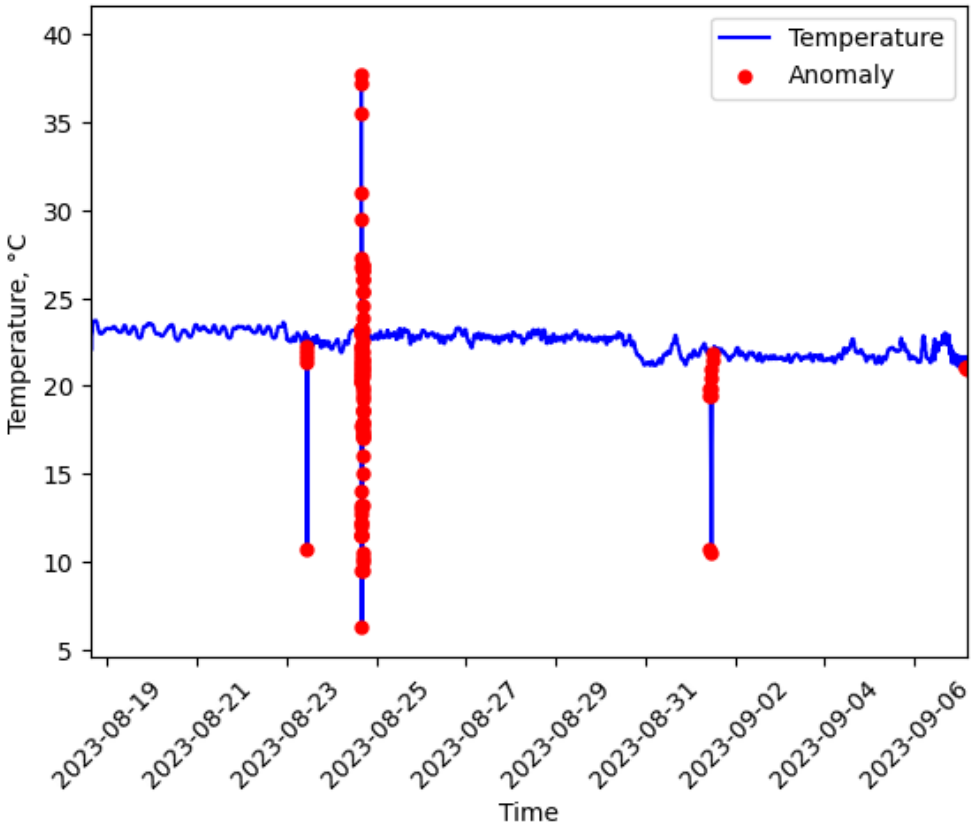

Figure 4.5: The plot shows the temperature sensor data collected by the CRFID sensor network. The anomalies detected are represented in red.

The efficient transmission of data is crucial. Under estimations that each data sample occupies 1 byte, with an associated energy cost of 0.01 mJ per byte for transmission, the total energy requirement to transmit all 3,595 samples (comprising 3,415 normal and 179 anomalies) is approximately 35.94 mJ. If only the 179 anomalous samples detected with the LSTM algorithm are transmitted, the energy consumption significantly drops to about 1.79 mJ, thereby achieving a substantial reduction in data transmitted by approximately 95.02%. With the operations performed near the sensors, this reduces latency, avoids delays in real-time detection, and reduces power from processing and transmitting large amounts of raw data to the cloud.

Chapter 5

VCRFID Tools for IoT Sensing Applications

At the same time, we developed the hardware of the VCRFID system tags; we designed an application and firmware to wirelessly program and send the instructions that control the operations of the RF IC and sensors. For the tags to interact with the reader hardware, the development software was required to handle the high-level commands and the firmware to convert them into low-level instructions that the reader board could understand. This application fulfills wirelessly and dynamically through the RF channel the configuring functions that, for example, other CRFID devices complete before deployment through a 4-wire programmer on the MSP430 to control access to the sensor. Analyzing the capabilities of typical RFID systems, we first encounter that the commercial reader technology, predominantly designed for warehouse inventory management, is constrained to three basic functions: select, inventory, and access [70]. This last function, access,

allows the user to read and write words from a specific register in the memory bank of the RFID IC. Therefore, recognizing the limitations of such a restricted functionality, we developed our own application, leveraging cutting-edge STMicroelectronics reader technology together with the EPC Gen2 protocol, to introduce a versatile solution tailored to meet the evolving needs of IoT and Industry 4.0.

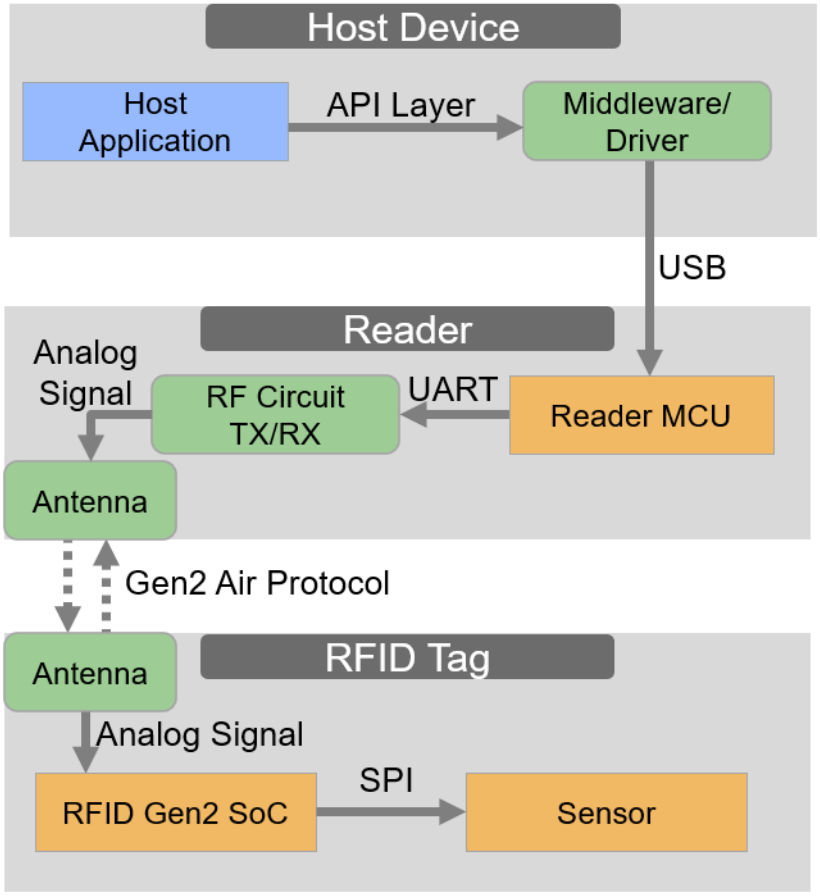

Figure 5.1: VCRFID system components and operation overview

5.1 Host and Reader

We pair the operation of a host computer and reader to handle the implementation of the EPC Gen2 standard for the UHF passive RFID system. The EPC Gen2 (v3) protocol offers features with commands for direct tag instruction, such as controlling the SPI bus that connects the sensors, broadening the scope of possible applications. EPC Gen2 is an air interface protocol defined by EPCglobal identified as the standard for UHF passive RFID (RAIN RFID) [71]. Part of the Gen2 protocol's focus is on enhancing the RFID system's security and overall performance in tune with Industry 4.0.

The VCRFID system, as previously introduced in Chapter 3 and Chapter 4, enables wireless identification and sensing using the VCRFID system tags hardware.

Based on the initial setup described, the system consists of three main components: the host, the reader (also known as an interrogator), and the RFID tag. These three elements interface together through the Rust code ecosystem, the program used for developing the software components of the VCRFID system. The following section contains a detailed description of each component and the operation of the VCRFID system.

As shown in Fig. 5.1, the host computer interfaces with the ST25RU3993 reader hardware through a dedicated software and firmware layer, which translates high-level commands into low-level instructions that the reader board can understand. This allows users to concentrate on developing application logic that incorporates the RF operations. The host computer manages key functionalities, including configuration management, sensor data processing, integration of ML processing,

and network communication, which are detailed as follows:

- Configuration Management: The host computer is used to handle the ST25RU3993 RF reader board's configuration, such as RF power, modulation, and data rate, to optimize the system for various operational environments and tag types.
- Data Processing: Once the RF reader board receives data from RFID tags, it is relayed to the host computer that processes this information, performing actions such as data logging, analysis, and ML processing, triggering external systems.
- Network Communication: The host computer often serves as a gateway, enabling the RFID system to communicate with other systems and databases over a network and setting up the protocol for message transmission, which supports uses like real-time monitoring.

5.1.1 Reader Hardware

The reader hardware consists of the ST25RU3993 RAIN (UHF) from STMicroelectronics with an STM32L476RGT6 (Arm® 32-bit Cortex®-M4) MCU and a UHF RFID reader IC ST25RU3993 for high-performance execution of UHF RFID reading and writing functions. The reader has a tunable radio frequency from 840 to 960 MHz that can operate in continuous wave mode or modulated RF output and is controlled by a host device via a USB/UART bridge. Figure 5.2 shows the ST25RU3993 RAIN (UHF) board with the mentioned controlling circuit, power connections, one for the external power amplifier (PA) and micro-B USB connector for communication and power from the host computer, and two RF ports, ANT1 and ANT2, for antenna connection.

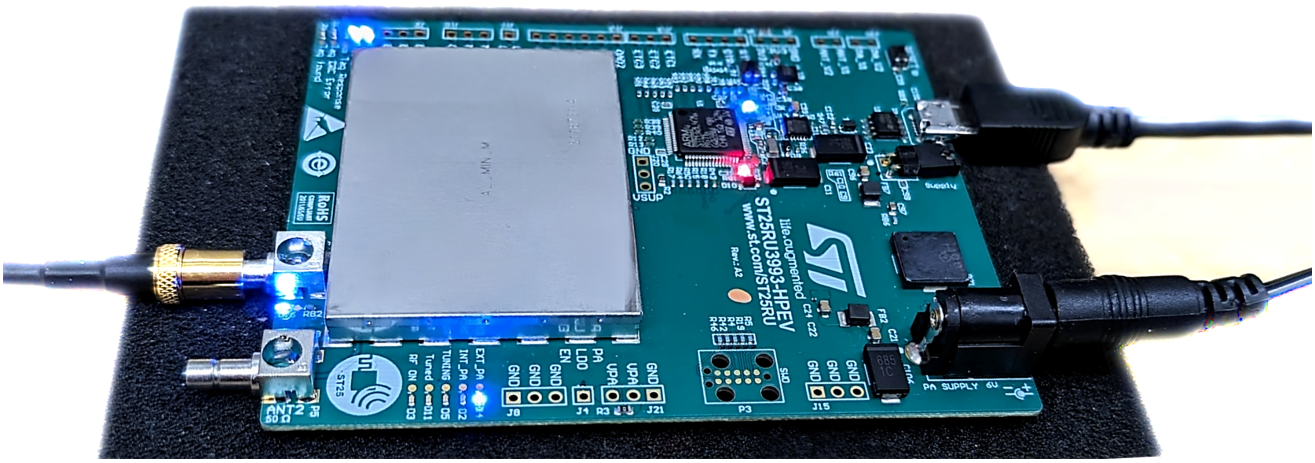

Figure 5.2: VRFID system reader ST25RU3993 RAIN (UHF) used for the RF communication, power, and control of the tags and embedded sensors

5.1.2 Reader Firmware

We developed a firmware to handle the control of the reader system and communicate with the RFID tags. This firmware handles the SPI and other custom commands through various crates and libraries, which include sensor libraries (adxl363) and a generic ST RFID library (libstuhfl). The app, in a RUST suite, covers a broad range of functionality, from basic sensor checks to configuration of the RFID IC and ADXL, demonstrating a thorough approach to validating tag interactions and sensor operations. The firmware code is available in the HPLP group repository.

Reading and Writing to the tag RFID SoC Memory

In order to read and write to the RFID SoC memory addresses, the RFID SoC has to be set to a specific reading mode in order to access the memory data. The configuration process involves writing to designated memory addresses within the user bank of the IC memory. For example, subsequent to the writing operation using the *em_write_config* test function, a verification read operation, *em_read_config*, can be conducted on the memory address to ensure the integrity of the data written and that the configuration of the tag IC was successful.

Memory Bank	Contents
1. Reserved	Kill password Access password
2. TID	48 bits fixed IC serial number
3. UII/EPC	352 bits UII/EPC encoding
4. User **(System memory)**	*Enable SPI* words and *control* words

Table 5.1: Memory bank layout. Gen2 tags have four banks of non-volatile memory: Reserved Memory, EPC Memory, Tag Identification (TID) Memory, and User Memory. Each of these memory banks is structured into 64 pages, with each page containing 4 words that are each 16 bits in length.

The memory of the RFID SoC is subdivided into four memory banks, as shown in Table 5.1, with

each of these memory banks structured into 64 pages, with each page containing 4 words that are each 16 bits in length. The first memory bank, defined as Reserved, contains the chip's Kill and Access passwords. The TID memory bank, containing the IC serial number that serves as the tag ID, is factory-configured and unmodifiable. The bits of UII/EPC encoding in commercial RFID tags serve as storage for the Unique Identifier for the tagged object. The user memory is allocated to the system memory configuration. Additionally, the user memory bank contains the words for passive and BAP mode configuration, as well as the I/O control words for the SPI enable mode, including interface configuration.

To list all available tests, from the host terminal, we can run: `cargo test -- --list`

To run a specific **test**, it can run using: `cargo test -- --show-output` **`test`**

Some of the main **`test`** functions for the tag SoC are:

- *continuous_power:* Controls the reader on/off of continuous power for the specified time. Supplies the tag RF power without interrogation.
- *find_tags:* Detect and identify tags within its range through a broadcast query for EPC ID.
- *em_passive_mode:* Configures the device's functionality in passive mode, utilizing internal power for operation without external sources like batteries.
- *em_bap_mode:* Configures the device's Battery Assisted Passive (BAP) mode for enhanced tag operation.
- *em_sensor_test:* Requests and retrieves the data of the temperature sensor integrated into the EM4325 device.

Reading Sensor Data

Once the tag device is configured as an SPI Master and SPI operation is enabled, the system reader can be used to send custom SendSPI commands to access sensor data. This approach enables the real-time acquisition of acceleration data for the interaction, for example, between the EM4325 chip and the ADXL363 accelerometer sensor. Nevertheless, as previously mentioned, this method requires the support of user-defined Gen2 commands by the RFID reader. A list of the operations enabled through the application functions, listed as serial Rust tests, is shown in Table B.1, and the main functions are described next.

Functions for the ADXL accelerometer sensor:

- *adxl_setup_config* This function sets the configurability of the ADXL device for optimal sensor performance.
- *adxl_sensor_test* Activates the functionality of the ADXL's sensors. Returns three axis acceleration data.
- *adxl_sensor_duration* Activates the functionality of the ADXL's sensors for a time specified. The ADXL sensor operates acceleration functions for a specific duration.

5.2 VCRFID from Edge to Cloud Implementation

For RFID-enhanced automated monitoring, we created a Python script that establishes the connection to an MQTT broker through a client application, reads RFID tag data from a reader or a series of readers, and then publishes the data to a specified MQTT topic. The database repository is connected to Grafana, an open-source platform for monitoring, visualization, and data analysis. It's designed to work with a specific RFID reader and MQTT broker configuration. MQTT is a network protocol that provides machine-to-machine publish-and-subscribe messaging. It was selected as the network protocol based on its lightweight implementation and bandwidth-efficient characteristics.

5.2.1 Automated Monitoring Features

Among the Features that the automated monitoring and reporting system integration performs are the following

1. Read tag data from an external reader using a sub-process for Rust Test.

2. Uses regular expressions to extract relevant information, metadata from the reader output.

3. Handles MQTT connection and credentials from host and publishing of data.

4. Connects to an MQTT broker to publish RFID tag data.

Chapter 6

High-sensitivity RF Energy Harvesters

6.1 Motivation

The sensitivity of the Radio Frequency Integrated Circuit (RF IC) impacts the operational efficacy of Radio Frequency Identification (RFID) systems. Specifically, it relates to the maximum distance at which an RFID reader can reliably communicate with an RFID tag. Enhanced sensitivity in the RF IC can facilitate operation over extended distances, potentially increasing the range, vital for applications requiring long-range wirelessly- powered devices, where increased sensitivity can lead to more robust and efficient operations.

One of the main questions is to find the design elements that make an effective harvester suitable for different input voltage ranges and dynamic loads. As we move farther from the source, the intensity of radio waves diminishes proportionally to the inverse square law; this poses a challenge due to the resulting limited input power. Another question in designing a high-sensitivity rectifier is that each component introduced to the harvester increases its total power usage. Thus, it's essential

for the rectifying stages to consume minimal power. Beyond reducing the power consumption of individual elements, what strategies can optimize the entire design to lower idle power consumption? Additionally, the choice of rectifier technology (e.g., Schottky diodes, deep N-well CMOS, zero V_{Th} transistors) affects the efficiency of RF signals conversion into DC power that satisfies the minimum operational threshold.

6.2 State of the art on RF harvesters

Previous research has explored the use of RF rectifiers as power supply for battery-less wireless devices since UHF RF energy is readily available for wireless communication. However, due to the limits on the transmitted power, as previously stated, rectifier sensitivity to low input power levels is key to achieve extended operating range of wirelessly-powered devices a critical aspect in their application. Additionally, a low input power tied to lossy elements in the matching circuit lead to smaller rectifier conversion efficiency.

Various designs that achieve a high sensitivity and good power conversion efficiency have been proposed. Noghabaei et al. in [72] present a novel ultra-low power rectifier designed for RF energy harvesting using 130nm CMOS technology and operating within the 915 MHz band. An off-chip differential matching network passively amplifies the incoming AC signal, followed by a self-compensated cross-coupled rectifier composed of 10 stages. This rectifier utilizes both dynamic and static bias compensation to minimize the forward voltage drop across transistors. Post-layout simulation results show a sensitivity of -30.5 dBm for generating 1 V output at a capacitive load.

Moreover, the rectifier achieves a peak end-to-end efficiency of 42.8% at -16 dBm input power, delivering 2.32 V at a 0.5MΩ resistor load. Kang et al. [73] in 2018 presented a bootstrapped rectifier–antenna that reuses the first stage of the rectifier and the antenna to boost the rectifier's output voltage. The two topologies presented, cross-coupled (CC) and cross-coupled pMOS (CP), enhance the rectifier output voltage without additional off-chip components. The CC topology which has commonly being used in other papers achieves an input sensitivity of -34.5 dBm, while the CP topology achieves - 26.5 dBm input sensitivity. Wu et al. in their 2021 article [74] report post-layout simulation results with a power conversion efficiency (PCE) of 27.6% at an input power level of -30 dBm at a 1MΩ resistance load. The output voltage reported are 525 mV for 1MΩ and an output voltage of 800 mV at capacitive load ($RL = \infty$) under a -30 dBm input power.

Previous works have incrementally pushed the boundaries of RF rectifier efficiency and sensitivity. It is evident from the previously cited designs that the challenge of optimizing these devices for broader and more efficient energy harvesting is both complex and multifaceted.

In the next section, we introduce a feedback self-adaptive body biasing rectifier that introduces a novel mechanism to further optimize RF energy harvesting, setting a new benchmark for sensitivity and power conversion efficiency in the 915 MHz band.

6.3 Body Biasing-based RF-DC Rectifier

We propose a novel feedback self-adaptive body biasing rectifier for RF energy harvesting for the UHF band (902-928 MHz). To ensure the received harvested energy is efficiently converted from RF to DC and enough to power the RFID IC and sensor circuit, we strive not only for a highly sensitive device but also for a large PCE. Based on 22nm fully-depleted silicon-on-insulator (FDSOI), the proposed 5-stage rectifier exhibits a high sensitivity of -31.4 dBm at 1V under a capacitive load, surpassing comparable results achieved by previous works. A good peak power conversion efficiency (PCE) of 31.3% under a 5MΩ load makes our rectifier ideal for ultra-low power RF energy harvesting. My contributions to this work included analyzing different designs, defining the methodology and reviewing the design.

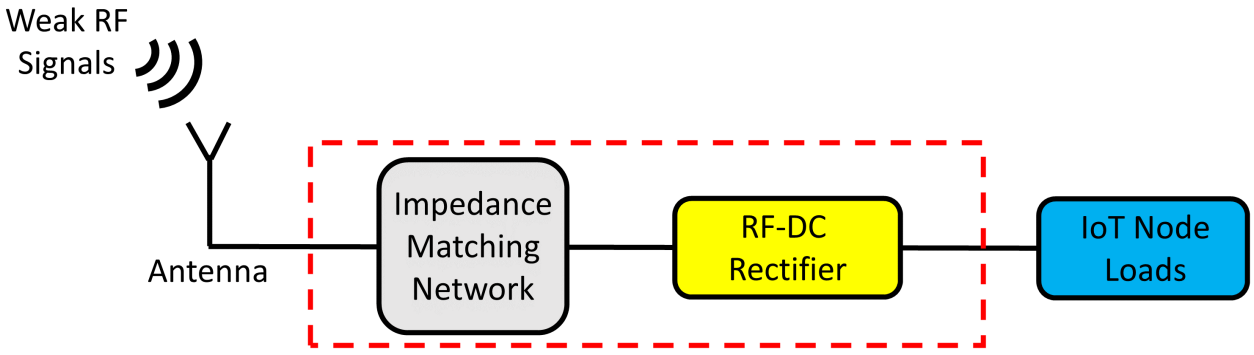

Figure 6.1: Diagram of RF energy harvesting front-end system

6.3.1 Impedance Matching Network

For the proposed IMN design, it is assumed that the impedance of an off-chip antenna is ideal as an RF voltage source, i.e., 50Ω. We choose a differential L-IMN structure because of its two advantages [75, 76]: i) boosting the small input voltage for the input of the rectifier and ii) minimizing the power reflection to maximize the input power transmission. Therefore, a well-designed IMN is necessary to achieve a high sensitivity for the rectifier for a given amount of low power.

The equivalent circuit of the RDR schematic with the IMN, the RF voltage source (V_{ANT}), and impedance (R_{ANT}) is shown in Fig. 6.2 (a). We note that the resistance of the RDR (R_{RDR}) and the capacitance of the RDR (C_{RDR}) change with the input voltage (V_{RDR}) of the RDR due to the nonlinearity of the circuit, thus it is worth investigating the changes in the impedance (Z_{RDR}) of the RDR corresponding to the changes of the amplitude V_{RDR} in order to determine the optimal values of the two inductors (L_{M1} and L_{M2}) and of the shunt capacitor (C_{M}) in the differential L-IMN. To investigate Z_{RDR}, R_{RDR}, and C_{RDR}, harmonic balance analysis is used by applying an RF voltage source (V_{RDR}) directly to the RDR. The Z_{RDR} can be derived from dividing Fast Fourier transforms (FFTs) of input voltage with FFTs of the input current in the frequency domain [77, 78], and then C_{RDR} and R_{RDR} are derived as below:

$$C_{\text{RDR}} = \frac{Im(\frac{I_{\text{RDR}}(\omega)}{V_{\text{RDR}}(\omega)})}{\omega} \tag{6.1}$$

$$R_{\text{RDR}} = \frac{1}{Re(\frac{I_{\text{RDR}}(\omega)}{V_{\text{RDR}}(\omega)})} \tag{6.2}$$

where $V_{\text{RDR}}(\omega)$ and $I_{\text{RDR}}(\omega)$ are the FFTs of input voltage and input current of the RDR at the required frequency, respectively.

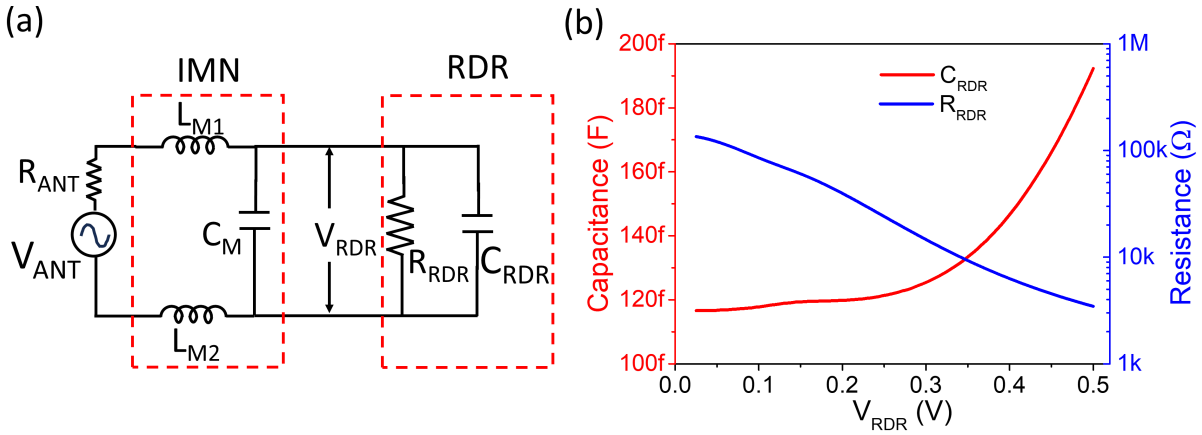

Figure 6.2: (a) Equivalent circuit of the design. (b) Characteristics of C_{RDR} and R_{RDR} under different V_{RDR}s.

Fig. 6.2 (b) shows the variation tendencies of both C_{RDR} and R_{RDR} of the proposed RDR under different V_{RDR}s. As the V_{RDR} is very small, the R_{RDR} is high, and C_{RDR} is low because the transistors are in the cut-off region. When V_{RDR} increases further, the C_{RDR} increases slowly while the R_{RDR} begins to decrease because the transistors are in the weak inversion region. As V_{RDR} increases to a large voltage, C_{RDR} increases rapidly while the R_{RDR} decreases further because the transistors are in the strong inversion region. Since the V_{RDR} is a boosted voltage amplitude passed by differential L-IMN [75, 79], it can be calculated as shown below:

$$V_{\text{RDR}} = G_{\text{bst,V}} \cdot V_{\text{ANT}} \tag{6.3}$$

where, $G_{\text{bst,V}}$ is the voltage gain boosted by the L-IMN. The absorption method is employed to

design the differential L-IMN. The IMN design starts with a typical L-type IMN where the C_{RDR} is absorbed as a shunt C_{total} while the inductor L_{M} is serially connected. Since the quality factor Q will be the same during series (parallel)-to-parallel (series) conversion, by equalling Q the relationship between the series reactance ($X_{\text{s}} = 2\pi f L_{\text{M}}$) and parallel reactance ($X_{\text{p}} = 2\pi f C_{\text{total}}$) will be: $X_{\text{s}}/R_{\text{ANT}} = R_{\text{RDR}}/X_{\text{p}}$ to determine both C_{total} and L_{M}. The C_{RDR} then needs to be subtracted from the C_{total} to obtain the C_{M}. Finally, the L_{M} can be considered as two series inductors (L_{M1} and L_{M2}) with the same inductance. Therefore, the closed-form of C_{M}, L_{M1}, and L_{M2} are given as below:

$$C_{\text{M}} = \frac{Q}{2\pi f R_{\text{RDR}}} - C_{\text{RDR}} \tag{6.4}$$

$$L_{\text{M1}} = L_{\text{M2}} = \frac{R_{\text{ANT}} Q}{4\pi f} \tag{6.5}$$

where Q is the quality factor of the IMN, which can be calculated as below:

$$Q = \sqrt{\frac{R_{\text{RDR}}}{R_{\text{ANT}}} - 1} \tag{6.6}$$

6.3.2 RF-DC Rectifier Design

Fig. 6.3 shows the proposed topology of the entire RF energy harvesting front-end system for high sensitivity. The antenna is assumed to be a sinusoidal voltage source. The received RF signals are passed to a proposed 5-stage RDR to rectify a very small RF signal to a large DC voltage above 1V.

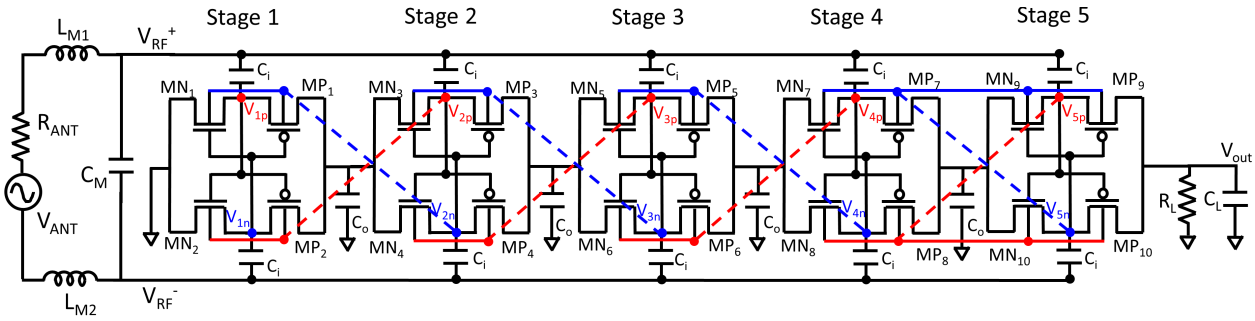

Figure 6.3: Proposed 5-stage RDR design with differential L-IMN

As shown in Fig. 6.3, the topology of the RDR is similar to the cross-coupled structure [80] to bias the gate of each transistor dynamically; thus, the opposite-phase RF potentials can be rectified. In the traditional cross-coupled topology, the body of each transistor is biased conventionally to a fixed voltage.

When the differential voltage input is in the positive region, one pair of NFET and PFET in each stage turns on to rectify the positive signal, while another pair in each stage turns on to rectify the negative signal when the differential voltage input is in the negative region. Using dynamic gate voltage to compensate V_{th} in the traditional cross-coupled RDR will help improve the efficiency of the rectifier. However, the sensitivity limitation of the RDR is the V_{th} of the transistor itself. In other words, the RDR will fail to rectify the input voltage much lower than the V_{th} of the transistor, especially in the extreme scenario where the available sensing power is very low, i.e., less than -20dBm. Such a dynamic gate voltage compensation strategy is not enough to overcome the sensing bottleneck for ultra-low-power RF energy harvesting. Therefore, we propose implementing feedback self-adaptive body biasing to enhance the traditional cross-coupled structure.

In Fig. 6.3, all transistors labeled with MN_n are N-type field effect transistors (NFETs) with super-

low-V_{th} and all transistors labeled with MP_n are P-type FETs (PFETs) with ultra-low-V_{th}, this is for making the initial V_{th} low. However, the initially low V_{th}s are still higher than our targeted ultra-low-power inputs; for example, V_{th} of the super-low-V_{th} NFETs is above 200mV. Thus an additional body biasing is used to reduce the V_{th} further to improve the sensitivity as the relationship between the V_{th} and the body biasing [81] is shown below:

$$V_{\text{th}} = V_{\text{th,0}} + \gamma(\sqrt{|\phi_\text{s} + V_{\text{sb}}|} - \sqrt{|\phi_\text{s}|}) \tag{6.7}$$

where $V_{\text{th,0}}$ is the threshold voltage when source biasing is equal to body biasing, V_{sb} is source-body voltage potential, γ is body effect coefficient, and ϕ_s is surface potential at the threshold. From the equation (6.7), we observe that forward body bias decreases the threshold voltage $|V_{\text{th}}|$ for both NFET and PFET, whereas reverse body bias increases $|V_{\text{th}}|$ for both FETs.

It is important to note that the signal is successively accumulated and amplified as it passes through each stage, progressing from node $V_{1\text{p}}$ to $V_{5\text{p}}$ for V_{RF}^{+} and from $V_{1\text{n}}$ to $V_{5\text{n}}$ for V_{RF}^{-}. Thus, the general idea of using feedback self-adaptive body biasing is in stage 1, when MN_2 and MP_1 turn on to rectify the positive input bias, the forward body biasing needs to be applied accordingly, i.e. applying $V_{2\text{p}}$ from the stage 2 to the body of MN_2 and applying $V_{2\text{n}}$ from the stage 2 to the body of MP_1. When MN_1 and MP_2 turn on to rectify the negative input bias, $V_{2\text{p}}$ from the stage 2 should be applied to the body of MN_1 and $V_{2\text{n}}$ should be applied to the body of MN_2. Except for the last stage, where the bodies should be fed within the stage ($V_{5\text{p}}$, $V_{5\text{n}}$) due to no next stage, the feedback body connection for the other stages is the same as the first stage. Such a body biasing method can be achieved using flipped-well transistors [82].

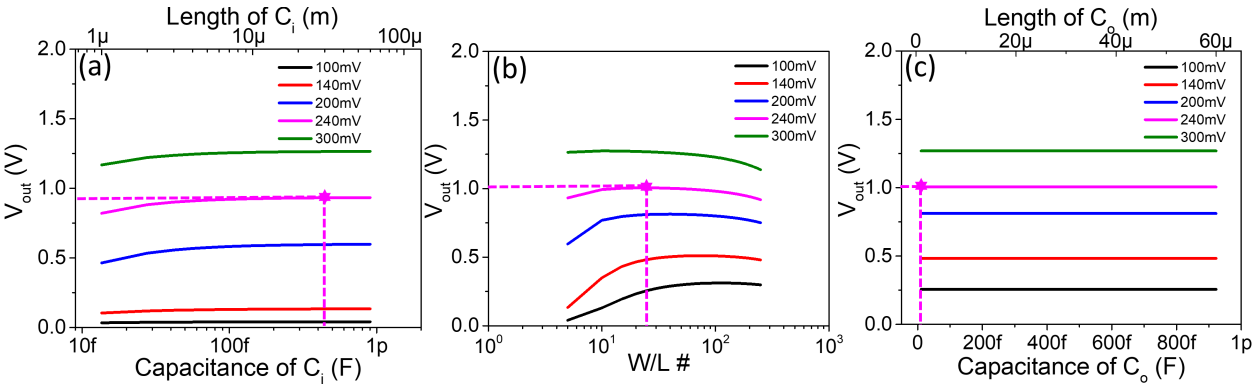

Figure 6.4: V_{out} with respect to (a) C_{i}, (b) W/L, and (c) C_{o}.

To achieve a voltage output equivalent to 1V at an ultra-low input power, as shown in Fig. 6.4, we select the capacitance of input capacitors (C_{i}), the width-length ratio (W/L) of NFET of the transistors, and output capacitors (C_{o}), and number of stages (N) in the RDR at their optimal values. A fixed capacitor width of 5μm, a resistive load of 10MΩ, and a capacitive load of 1pF will result in outputs of 1V. The width of the PFETs is chosen twice that of the NFETs. Each parameter was swept from its minimum value to the allowed maximum value.

We propose a control variable method to discover optimized parameters in the order of C_{i}, W/L, C_{o}, and N. In general, for a fixed N, the V_{out} of RDR increases with increasing input voltage amplitude, but it changes differently when varying the first three parameters mentioned above.

In Fig. 6.4 (a), the V_{out} increases with C_{i} but then saturates with further increasing C_{i}. In Fig. 6.4 (b), the V_{out} increases with W/L and then decreases when increasing W/L over 25 for given C_{i} because of the increasing reverse leakage from the output. In Fig. 6.4 (c), given an input voltage amplitude, the V_{out} remains constant with increasing C_{o} when fixing both C_{i} and W/L, so we optimize the C_{o} in its minimum size to minimize the RDR area. From (6.3), the antenna output

voltage can be amplified to ∼240mV, so the C_{i}, W/L, and C_{o} are optimized and labeled in Fig. 6.4 as 458fF, 25, and 13.5fF for the proposed optimized design.

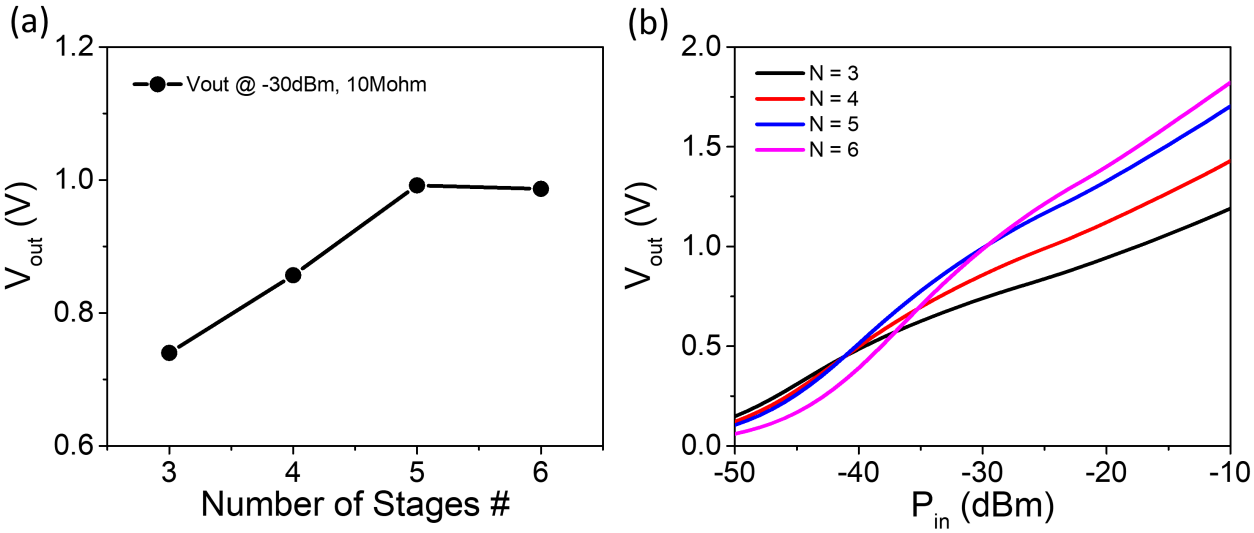

Figure 6.5: The V_{out} under different (a) number of stages and (b) input power.

To discover the optimal N, the V_{out}s of RDR with the proposed structure across four different stages was studied. Before the comparison, the component parameters of each proposed RDR with different stages were optimized using the above-proposed methods with corresponding IMNs. In Fig. 6.5 (a), for a fixed input power and load, the V_{out} increases with N, but it starts to decrease after $N > 5$. This is because more stages will introduce more capacitors, degrading the sensitivity with reverse leakage [83] and additionally causing area overhead. In Fig. 6.5 (b), V_{out} of RDR increases with input power. The 5-stage RDR shows higher V_{out} than that of RDRs with fewer stages. With an input power lower than -30dBm, our RDR design can output 1V. Therefore, the optimal N is chosen to be 5.

6.3.3 Simulation Results

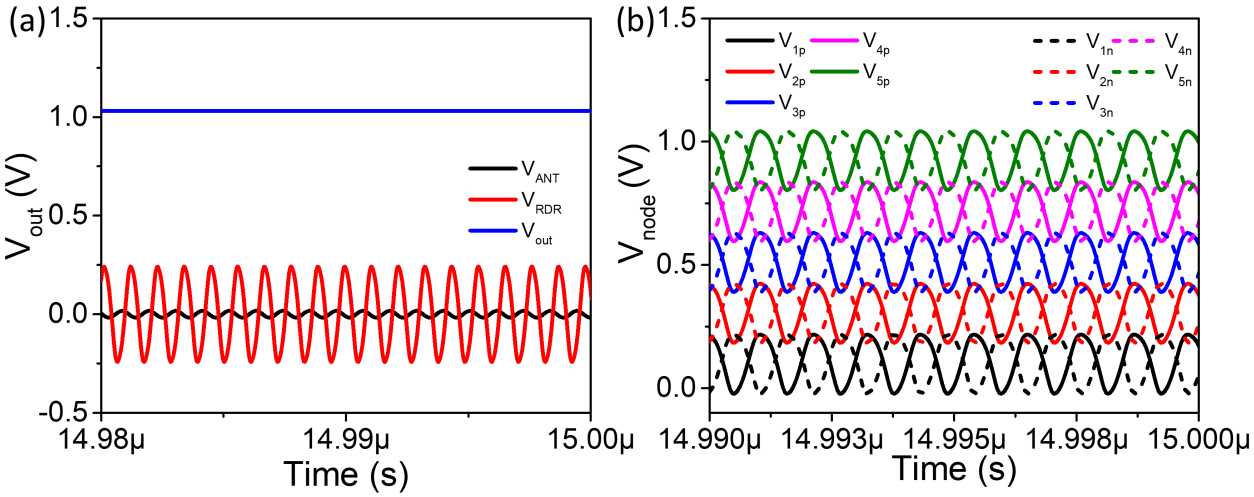

Figure 6.6: Transient responses of (a) nodes from V_{1p} (V_{1n}) to V_{5p} (V_{5n}) and (b) V_{out} under different loads of the proposed design.

The proposed 5-stage RDR design was simulated using a commercial 22nm FDSOI technology. The flipped-well technique of NFET and PFET can achieve forward body biasing. The targeted input central frequency is 915MHz based on the industrial, scientific, and medical (ISM) band (902-928 MHz). The estimated area is around 0.00194mm^2 since most of the area is occupied by capacitors. Fig. 6.6 (a) shows the proposed RDR output DC voltage of 1.02V at -30dBm input power under a capacitive load. The differential input voltage amplitude V_{ANT} is amplified by the proposed differential L-IMN from 17mV to V_{RDR} of 242mV, which is similar to the amplification effect in [75]. Fig. 6.6 (b) shows the voltage amplifications on the nodes of each stage, i.e., from node V_{1p} to V_{5p} and from node V_{1n} to V_{5n} with 180-degree phase differences.

In Fig. 6.7 (a), V_{out} of the proposed RDR was investigated across different input power under varied

resistive loads and corners. Corner simulation is performed under 10MΩ. The V_{out} increases with input power and load resistance. The proposed 5-stage RDR achieves a high sensitivity of -31.4dBm to output 1V under a capacitive load at a typical-typical (TT) corner, which shows the capability to operate at ultra-low input power for energy harvesting. Fig. 6.7 (b) shows the evaluation of peak PCEs of the proposed RDR at different loads, corners, and temperatures when input power varies from -50dBm to -10dBm. The PCE is calculated as output power over input power. It can be seen that the overall maximum peak PCE at TT corner is 31.3% (-38dBm at 5MΩ). The peak PCE is still above 20% when input power varies from -41dBm at 10MΩ to -28dBm at 1MΩ, suggesting the capability of ultra-low power energy harvesting with competitive PCEs.

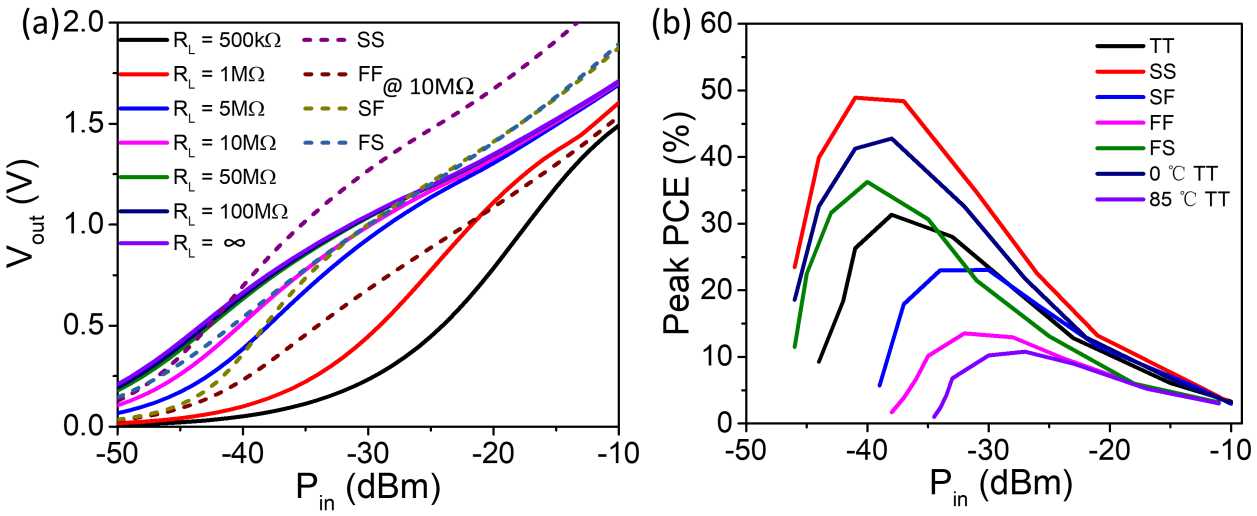

Figure 6.7: (a) V_{out} under different loads and corners and (b) peak PCEs under different loads, corners, and temperatures

However, both V_{out} and the peak PCEs are affected by process variations and temperatures when the input power is very low. This is because the V_{th}s of transistors at advanced technology nodes are very sensitive to random doping fluctuations [84] and temperature variations [85]. For future

work, we will implement DC-DC converter-related circuits to vary loads to track the maximum power point and strengthen variation resilience at the next stage.

Table 6.1: Simulation comparison among cross-coupled rectifiers

Reference	**Noghabaei 2018 ISCAS [75]**	**Wu 2021 ISCAS [76]**	**Al-Absi 2021 ACCESS [81]**	**Lian 2021 APCCAS [86]**	**Yin 2024 ISCAS *This work***
Technology	130nm	130nm	180nm	65nm	22nm
Frequency	915MHz	915MHz	953MHz	900MHz	915MHz
Structure	Self-compensated	Self-bias	Body biasing	Xformer	Feedback body biasing
Stages (N)	10	6	5	5	5
Extra circuitry	No	Yes	No	Yes	No
Variation analysis	No	No	No	No	Yes
Peak PCE	42.8% @ -16dBm	27.6% @ -30dBm	78.2% -27.5dBm	- NA -	31.3% -38dBm
Sensitivity ($R_L = \infty$)	-30.5dBm @ 1V	-30dBm @ 800mV	-7.1dBm @ 1V	-17.8dBm @ 1V	-31.4dBm @ 1V

Table 6.1 shows the simulation-based performance comparison between state-of-the-art cross-coupled RDRs and our proposed RDR. We use TT corner results to make a fair comparison since other works did not perform variation analysis. Although [81] shows a high peak PCE at -27.5dBm, it assumes a perfect impedance matching, the V_{out} at that power is below 0.5V, while the V_{out} of the proposed design is above 0.6V at the similar peak PCE power. The proposed RDR in this section shows the highest sensitivity of -31.4dBm with the least number of stages and no extra circuitry.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

Internet of Things (IoT) has emerged, integrating everyday physical objects into a smart, interconnected network. This digital cyber-physical revolution, driven by the demand for connectivity and information, has been accelerated by wireless devices enabling remote communication, control, monitoring, and automation. As we navigate the challenges of power delivery and data management in the vast and multifaceted IoT landscape, the role of Radio Frequency Identification (RFID) becomes increasingly significant, especially in the context of Industry 4.0.

This dissertation presents a unique approach to wireless sensing IoT devices through computational RFID technology, combining RFID capabilities with advanced computational and sensing technology.

This work is driven by the potential of smart sensing devices based on RFID technology and the tangible benefits they can bring. Known for its low cost, simplicity, and efficiency, the VCRFID sensor system offers practical solutions to predict industrial equipment failures using real-time data and historical machine behavior analysis. By simplifying the implementation and deployment of computational RFID systems for equipment monitoring and predictive maintenance, we can significantly reduce downtime and maintenance costs, thereby contributing to the advancement of smarter, more connected factories.

Affordability and adoptability

- Affordability

The circuit design introduced in this work significantly lowers the cost of the tag to approximately $14USD, representinganearly$10 USD reduction compared to previous CRFID implementations. This substantial cost reduction highlights the proposed design's economic advantage. Moreover, we can compare the costs of implementing VCRFID systems against the benefits, such as operational efficiency and the cost savings over time from failure detection using the sensors.

- Adoptability

In terms of how easily a new device or system can be integrated or accepted by users, the simplicity of the VCRFID system tags and the high degree of automation, flexibility, and reconfigurability sustain the devices' adoptability. Among the challenges, the percentage of acceptance by end-users is tied to the initial setup costs of the system. However, these costs can be effectively offset by the scalability of the system, which supports a large number of VCRFID sensing

devices (Max. 700 tags/s), making larger implementations economically viable. Another possible adoptability challenge is compliance with industry regulations and standards that influence acceptance rate, particularly in highly regulated sectors such as the military and associated with security compliance.

Our contributions to this field are various; we enhance sensor tags from mere data collectors to intelligent autonomous systems that leverage RF for sensing, computing, and self-powering, thus enabling real-time data accessibility from anywhere. By focusing on designing and fabricating sensing tags and developing custom reader firmware, we facilitate the full integration of a VCRFID sensor system.

Moreover, the exploration of Machine Learning at the edge and the implementation of Wireless Sensor Networks (WSN) with edge data processing and cloud integration hold immense potential for optimizing data analysis and decision-making processes. In summary, this thesis lays the groundwork for a more efficient computational RFID for predictive maintenance. It presents an innovative approach that addresses the power challenges of IoT and highlights the critical role of advanced wireless technologies based on RFID in driving the transformation for a more sustainable future. The following section outlines the specific contributions of our research.

7.1.1 Contributions

1. The design and fabrication of a new type of ultra-low power sensing tags, where the innovation is achieved through a microcontroller-free design approach, combining UHF RF energy harvesting and sensor integration into an energy-efficient battery-less sensing RFID tag design for the VCRFID system.

2. The development of new reader applications and firmware based on the ST25Ru3993 board from STMicroelectronics as the reader hardware of the VCRFID sensor system. The firmware supports the EPC-Global Class 1 Gen-2 UHF RFID Standard, which establishes a virtualized controller for SPI-over-RF, enabling seamless communication and control over the tag devices. The system integrates RF energy harvesting and wireless sensor control, increasing efficiency and expanding the scope of RFID technology in sensing applications. Additionally, the software app facilitates the interaction between the host computer and the RFID reader to manage UHF passive RFID systems effectively.

3. The implementation of Wireless Sensor Networks (WSN) with edge data processing reduces latency and minimizes transmission costs in a sensor-to-cloud architecture. This approach keeps data in proximity to its source, reducing transmission costs and delays in real-time anomaly detection applications.

4. The combination of the VCRFID system with machine learning techniques for conducting ML analysis, specifically targeting temperature sensing applications aimed at remote monitoring and applications oriented to equipment predictive maintenance.

5. We introduce an enhanced RDR RF harvester design with a sensitivity of -31.4 dBm and a power conversion efficiency of 31.3%. The proposed design enables longer-range operations that could significantly increase the operational reach of the VCRFID system beyond previously reported distances.

6. A framework for the research, design, and development of CRFID prototypes that can be extended beyond Industry 4.0 scenarios. It includes a suite of development tools and libraries to streamline the design, testing, and creation of new applications. Additionally, the framework supports iterative optimization processes, ensuring compatibility and functionality across various hardware platforms.

7.1.2 Research Impact and Implications of the work

To quantify the impact and implications of our research in Computational RFID, we consider the following points:

1. **Cost Reduction:** Through a more straightforward design that eliminates the need for microcontrollers embedded on the tag circuit to manage the sensors, we estimate a notable cost reduction of approximately $10 USD per Computational RFID tag. Additionally, the VCRFID system completely removes the need for ongoing device maintenance associated with battery replacements.

2. **Energy Consumption Reduction:** With the implementation of the VCRFID sensing system, we observe a 97% energy consumption reduction compared to computational tags with

MCUs. In addition, we see improvements in data transmission efficiency by 95% by only transmitting anomalies detected using the ML method.

3. **Adoption Rate:** By comparing the current number of users of RFID systems across various industries, we can anticipate a significant uptake of the new VCRFID technology. VCRFID is an attractive IoT option driven by the ease of implementation of the sensing devices, lower costs per device, and enhanced self-power capabilities.

7.2 Future Work

Based on the work of this dissertation, two primary avenues for future research are identified. The first is related to the security of the VCRFID system, where we have found encryption methods, such as the Advanced Encryption Standard (AES), difficult to implement on the constrained memory and power resources of the VCRFID system tags. A second avenue of research is an optimized ML model for vibration anomaly and predictive maintenance. An unsupervised method that can match anomalies from any machinery in different scenarios involves the development of algorithms capable of learning from unlabeled data, identifying patterns, and distinguishing between normal operation and failure. In this work, we have proposed and put into operation a system that employs a Virtualized Controller for Computational RFID-based IoT Sensors [44] and the use of power at the edge to enable the smart sensing and computational capabilities of the VCRFID system [87]. We have used the VCRFID system as a Wireless Sensor Network (WSN) with edge data processing based on an LSTM autoencoder in the host device (raspberry Pi) that minimizes transmission costs to the cloud. The next improvements should focus on continuing the exploration, incorporating VCRFIDs and Machine Learning at the edge, and refining data preprocessing for ML analysis.

The security aspect is particularly significant in the future research topics identified in this dissertation. The following section describes this subject in more depth, examining the current challenges and future directions for enhancing the security mechanisms of VCRFID systems. Addressing these concerns is essential for facilitating a trustworthy deployment across various operational settings.

7.2.1 CRFID Security: Threats and Defense

The existing VCRFID system supports password protection of the read and write functions to access and kill the RF IC. However, to effectively prevent security breaches, the system will require more robust security measures. Strengthening security functions increases the resilience and dependability of applications and ensures trustworthiness and user privacy. This section first examines various potential security threats to the VCRFID system. Following this, it presents an overview of recent advancements in security solutions that address these threats, setting the stage for introducing our innovative approach designed to fortify the security of VCRFID applications further, ensuring they are more robust and reliable.

Types of CRFID Threats

Understanding the potential threats to RFID systems is crucial for implementing robust security measures. We list several types of attacks targeting RFID tags:

1. Eavesdropping and snooping: The exchanged information can be compromised if unauthorized interception of transmitted data between RFID tags and legitimate or unauthorized readers occurs [88].
2. Data tampering: Involves the unauthorized modification or deletion of information stored on RFID tags. This illegitimate modification can lead to malfunctions within the RFID tag or loss of information, compromising its operation and potentially disrupting its overall performance [19].
3. Unwanted access and password decoding: Unauthorized use of RFID systems by entities lacking proper authorization exploiting vulnerabilities or compromising the security and in-

tegrity of the system. This unauthorized use can lead to potential data breaches, system manipulation, or misuse of sensitive information [88].

4. Electromagnetic interference: The communication between tags and readers can be sabotaged, preventing exchange or interference with added noise, jamming, Denial of Service, or disrupting the RF field between reads and writes [88, 89].

CRFID Defense Against Security Threats

From the creation of the first CRFIDs, the primary concern has been creating methods to execute software capable of enforcing security protocols against unauthorized reads and encryption methods on the CRFIDs. Kevin Fu implemented an RC5 block cipher algorithm on the WISP, calling it "Maximalist Cryptography" since it represents a full-strength approach with plenty of computational capabilities [90]. Similarly, Pendl was able to implement elliptic curve cryptography (ECC) on the WISP MSP430 microcontroller [91]. At the same time, a diverging direction into minimalist or lightweight cryptography stemmed from the need for approaches to implement cryptographic protocols in resource-constrained passive RFID devices lacking power and computational resources.

Ciphers such as AES [90] and RC5 [92] can be implemented on the microcontrollers of the WISP, avoiding the time and expense of creating custom silicon for these functions. This type of robust algorithm requires tens of thousands of gate equivalents for implementation. However, a solution for RFID tags that do not have a microcontroller embedded can be completed through authentication methods and with the use of novel cryptography methods, which require to be demonstrated in ultra-constrained RFID devices with just thousands of gate equivalents [93, 94].

Impinj, one of the leading RFID providers, offers a highly reliable cryptographic tag authentication. The M775 RFID chips and the R700 series readers, in addition to their regular inventory functions, provide an added layer of security through the Impinj Authentication Service, ensuring the authenticity of the tagged product.

Together with password authentication and Physical Unclonable Functions (PUFs), a lightweight cipher or asynchronous encryption method could be implemented for VCRFID tags, where the reader could complete the data transmission security.

7.2.2 Cryptography on the VCRFID System

In the context of the VCRFID system, to secure the wireless channel between a reader and a passive RFID tag, we consider focusing on a lightweight encryption approach that leverages the reader's computation capabilities while minimizing the demands on the tag device. An ideal approach will balance security with the computational and energy constraints of passive tags, addressing challenges like power consumption, gate count, encryption time, and storage of sensitive data. A suggested technique is asymmetric public-key cryptography. Prior works have considered cryptosystems based on stream ciphers, such as the public-key cryptography method implemented by [95]. The Rabin Encryption variant WIPR is designed for use in passive RFID tags, which are typically limited in power and computational resources. Similarly, the lightweight encryption method PRESENT [96] is recognized for its efficiency and suitability for devices with limited resources. PRESENT is a lightweight block cipher for low power that supports key sizes of 128-bit,

catering to specific security requirements. It has been shown to consume fewer logic resources and power compared to conventional cryptography methods(AES-128), making it cost-effective for hardware implementation [97].

The proposed methodology is intended to align with a set of criteria designed to select an encryption method that balances resource utilization with security needs. Initially, the methodology involves identifying a lightweight encryption method, such as PRESENT [96, 97] or WIPR [95]. Following this, the selected encryption method should be simulated and synthesized onto an FPGA. Subsequently, integration with the RF IC of the VCRFID system is to be completed, followed by comprehensive testing. Ultimately, the methodology calls for a comparison of the performance of WIPR and PRESENT, as observed from software simulations against FPGA implementations, by analyzing performance metrics.

1. FPGA Design:
    (a) Translate the chosen encryption method (based on software analysis) into VHDL or Verilog for FPGA implementation.
    (b) Optimize the design to exploit the FPGA architecture, focusing on speed and resource utilization.
2. Simulation and Synthesis:
    (a) Simulate the FPGA design to ensure functional correctness.
    (b) Synthesize the design to map it onto the FPGA, paying attention to optimization for performance, area utilization, and power.

3. Integration with RF IC:

    (a) Develop the interface between the FPGA and the RF IC to ensure seamless communication.

    (b) Implement the necessary control software to manage the data flow and encryption/decryption processes between the FPGA and RF IC through an SPI interface.

4. Physical Testing:

    (a) Conduct field tests to evaluate the encryption system's performance in real-world RFID communication scenarios.

    (b) Measure the final system's power consumption, encryption/decryption time, reliability, and overall robustness to attacks.

In summary, the development of a reliable and energy-efficient cryptographic method tailored to the intended application and sufficiently compact to fit on an RFID tag can be achieved through the utilization of various hardware design optimization techniques. Furthermore, the system can be validated against reported performance metrics in previous works to ensure its readiness for deployment. With this methodology, we can identify a working cryptography method that meets the tag's power and area constraints and satisfies the speed requirements for the intended applications and security level.

Appendix A

List of Publications

A.1 Conferences

1. Mac Cartier, Rahul Sreekumar,**Elisa Pantoja**, and Mircea Stan. "Koch Curve Polar Coordinate Transform for UWB Antenna Applications." In 2022 8th International Conference on Antennas and Electromagnetic Systems

2. **Elisa Pantoja**, Rahul Sreekumar, Sergiu Mosanu, Tommy Tracy, and Mircea Stan. "Virtualized Controller for Computational RFID-based IoT Sensors." In 2023 IEEE International Conference on RFID (RFID), pp. 54-59.

3. **Elisa Pantoja**, and Mircea Stan. "Advancing Wireless IoT Sensor Networks With Edge-Powered RFID Devices." In 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference

4. Jun Yin, **Elisa Pantoja**, Yimin Gao, and Mircea Stan. "A Feedback Self-adaptive Body Biasing-based RF-DC Rectifier for Highly-sensitive RF Energy Harvesting" ISCAS 2024

A.2 Journals

1. **Elisa Pantoja**, Rajendra Bhatt, Anping Liu, Mool C. Gupta. "Low thermal emissivity surfaces using AgNW thin films." Nanotechnology. 2017 Nov 23;28(50):505708.

2. Joel T. Harrison, **Elisa Pantoja**, Moon-Hyung Jang, and Mool C. Gupta. "Laser sintered PbSe semiconductor thin films for Mid-IR applications using nanocrystals." Journal of Alloys and Compounds 849 (2020): 156537.

A.3 SRC TECHCON

- **Elisa Pantoja and Mircea Stan**, "Chipless and battery-less all inkjet printed RFID tag for temperature smart sensing." TECHCON 2021

- **Elisa Pantoja and Mircea Stan**, "High-efficiency compact antenna for on-metal RFID temperature sensing applications.", TECHCON 2022

A.4 Awards

1. **Best Presenter** Track III: Mobile Communication, Session 20, for the paper titled: “Advancing Wireless IOT Sensor Networks With Edge-Powered RFID Devices” at IEEE UEMCON’23

2. **Flash Talk** - Link-Lab Research Day Fall 2022 ”CRFID Sensors for Remote Monitoring”

3. **1st Place Young Researcher Roger Kelly Award** at the the 5th international School Lasers in Materials Science SLIMS’16 Awards

Appendix B

Reader Software and Firmware

The code developed is available in the HPLP repositories, which includes all source codes and documentation (see links for details)

HPLP GitHub

HPLP Drive.

B.1 Reader Test List

The following is a list of the operations enabled through the application functions, listed as serial Rust tests:

IC	Test	Description
RFID EM4325	continuous_power	Controls the reader on/off of continuous power for the specified time, supplies the tag RF power without interrogation.
	find_tags	Detect and identify tags within its range through a broadcast query for EPC ID.
	em_passive_mode	Configures the device's functionality in passive mode, utilizing internal power for operation without external source like batteries.
	em_bap_mode	Configures the device's for Battery Assisted Passive (BAP) mode for enhanced tag operation.
	em_pseudo_bap_mode	Set the device's functionality in a simulated BAP mode, balancing between passive operation and RF storage in a capacitor in between operations.
	em_write_config	Set the device's configuration writing the setting values to its memory.
	em_read_config	Reads back the device's configuration settings from its memory.
	em_sensor_test	Requests and retrieves the data of the temperature sensor integrated into the EM4325 device.
	em_verify_calibration	Confirms the accuracy of the device's calibration for temperature sensor readings.
Sensor ADXL362	adxl_read_test	Tests the ADXL device's ability to read sensor data accurately.
	adxl_write_test	Set the ADXL device's to write data or settings.
	adxl_setup_config	Set the configurability of the ADXL device for optimal sensor performance.
	adxl_sensor_test	Activates the functionality of the ADXL's sensors. Returns three axis acceleration data.
	adxl_sensor_duration	Activates the functionality of the ADXL's sensors. The ADXL sensor operate acceleration function for a specific duration.

Table B.1: Test items and descriptions for EM4325 and ADXL Devices

Glossary

Acronyms and Abbreviations	
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ASK	Amplitude Shift Keying
CLK	Clock Signal
CPU	Central Processing Unit
CRFID	Computational Radio Frequency Identification
CRISP	Center for Research on Intelligent Storage and Processing-in-Memory
ECE	Electrical and Computer Engineering
ECC	Elliptic Curve Cryptography
EIRP	Effective Isotropic radiated power
EPC	Electronic Product Code
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
HPLP	High-Performance Low-Power research lab at University of Virginia

IoT	Internet of Things
MCU	Microcontroller Unit
ML	Machine Learning
NFC	Near-field communication
PUF	Physical Unclonable Function
RC5	Rivest Cipher 5
RFID	Radio Frequency Identification
SPI	Serial Peripheral Interface
SRC	Semiconductor Research Corporation
UVA	University of Virginia
UHF	Ultra High Frequency
VCRFID	Virtualized Controller for Computational RFID
VCU	Virginia Commonwealth University
VHDL	VHSIC Hardware Description Language
WISP	Wireless Identification and Sensing Platform

Bibliography

[1] G. Scheible, D. Dzung, J. Endresen, and J. E. Frey, "Unplugged but connected [design and implementation of a truly wireless real-time sensor/actuator interface]," *IEEE Industrial Electronics Magazine*, vol. 1, no. 2, pp. 25–34, 2007.

[2] M. Luvisotto, F. Tramarin, L. Vangelista, S. Vitturi *et al.*, "On the use of lorawan for indoor industrial iot applications," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[3] M. Luvisotto, Z. Pang, and D. Dzung, "Ultra high-performance wireless control for critical applications: Challenges and directions," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1448–1459, 2016.

[4] L. Erhan, M. Ndubuaku, M. Di Mauro, W. Song, M. Chen, G. Fortino, O. Bagdasar, and A. Liotta, "Smart anomaly detection in sensor systems: A multi-perspective review," *Information Fusion*, vol. 67, pp. 64–79, 2021.

[5] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig,

"Requirements and current solutions of wireless communication in industrial automation," in *2014 IEEE international conference on communications workshops (ICC)*. IEEE, 2014, pp. 67–72.

[6] A. A. Bailey, I. Pentina, A. S. Mishra, and M. S. Ben Mimoun, "Mobile payments adoption by us consumers: an extended tam," *International Journal of Retail & Distribution Management*, vol. 45, no. 6, pp. 626–640, 2017.

[7] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (nfc) technology," *Wireless personal communications*, vol. 71, pp. 2259–2294, 2013.

[8] V. D. Hunt, A. Puglia, and M. Puglia, *RFID: a guide to radio frequency identification*. John Wiley & Sons, 2007.

[9] Wang *et al.*, "IEEE Council on Radio-Frequency Identification: History, Present, and Future Vision," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 170–175, 2020.

[10] Statista, L. Sujay Vailshery. (2023) Internet of Things (IoT) in the U.S. - statistics & facts. [Online]. Available: https://www.statista.com/topics/5236/internet-of-things-iot-in-the-us/

[11] Statista, Transforma Insights. (2022) Internet of Things (IoT) revenue worldwide from 2020 to 2030 (in billion U.S. dollars). [Online]. Available: https://www.statista.com/statistics/1183471/iot-revenue-worldwide-by-vertical/

[12] Statista-Transforma Insights. (2023) Internet of Things (IoT) total annual revenue worldwide from 2020 to 2030. [Online]. Available: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/

[13] Statista, L. Sujay Vailshery. (2023) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[14] S. R. Corporation. (2020) SRC Decadal Plan for Semiconductors Abridged Report. Accessed on November 06, 2023. [Online]. Available: https://www.src.org/about/decadal-plan/

[15] W. Wang, V. A. L. Sobral, M. F. R. M. Billah, N. Saoda, N. Nasir, and B. Campbell, "Low power but high energy: The looming costs of billions of smart devices," *ACM SIGENERGY Energy Informatics Review*, vol. 3, no. 3, pp. 10–14, 2023.

[16] A. Klinefelter, N. E. Roberts, Y. Shakhsheer, P. Gonzalez, A. Shrivastava, A. Roy, K. Craig, M. Faisal, J. Boley, S. Oh *et al.*, "21.3 a 6.45 μw self-powered iot soc with integrated energy-harvesting power management and ulp asymmetric radios," in *2015 IEEE International Solid-State Circuits Conference-(ISSCC) Digest of Technical Papers*. IEEE, 2015, pp. 1–3.

[17] J. Hester and J. Sorber, "The future of sensing is batteryless, intermittent, and awesome," in *Proceedings of the 15th ACM conference on embedded network sensor systems*, 2017, pp. 1–6.

[18] S. Gollakota, M. S. Reynolds, J. R. Smith, and D. J. Wetherall, "The emergence of rf-powered computing," *Computer*, vol. 47, no. 1, pp. 32–39, 2013.

[19] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 5772–5781.

[20] Deloitte. (2022) Predictive maintenance and the smart factory - Connecting machines to reliability professionals. [Online]. Available: https://www2.deloitte.com/us/en/pages/operations/articles/predictive-maintenance-and-the-smart-factory.html

[21] Polaris Market Research. (2022) Predictive Maintenance Market Share, Size, Trends, Industry Analysis Report. [Online]. Available: https://www.polarismarketresearch.com/industry-analysis/predictive-maintenance-market

[22] Presedence Research. (2024) Predictive Maintenance Market in the U.S. 2023 To 2032. [Online]. Available: https://www.precedenceresearch.com/predictive-maintenance-market

[23] P. Nikitin, "Guest editorial: Special issue on ieee rfid 2017 conference," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 1–2, 2017.

[24] Energous Corporation. (2023) Energous Breakthrough: FCC Approval for 15W WattUp. [Online]. Available: https://ir.energous.com/news-events/press-releases/detail/732/energous-breakthrough-fcc-approval-for-15w-wattup

[25] H. Westman, "Reference Data for Radio Engineers. Indianapolis: Howard W. Sams & Co," 1968.

[26] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[27] B. Fennani, H. Hamam, and A. Dahmane, "RFID overview," in *ICM 2011 Proceeding*. IEEE, 2011, pp. 1–5.

[28] J. R. Smith, *Wirelessly Powered Sensor Networks and Computational RFID*. Springer Science & Business Media, 2013.

[29] M. Buettner, R. Prasad, A. Sample, D. Yeager, B. Greenstein, J. R. Smith, and D. Wetherall, "RFID sensor networks with the Intel WISP," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008, pp. 393–394.

[30] J. R. Smith, K. P. Fishkin, B. Jiang, A. Mamishev, M. Philipose, A. D. Rea, S. Roy, and K. Sundara-Rajan, "RFID-based techniques for human-activity detection," *Communications of the ACM*, vol. 48, no. 9, pp. 39–44, 2005.

[31] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R. Smith, "Design of an RFID-based battery-free programmable sensing platform," *IEEE transactions on instrumentation and measurement*, vol. 57, no. 11, pp. 2608–2615, 2008.

[32] S. Milici, S. Amendola, A. Bianco, and G. Marrocco, "Epidermal RFID passive sensor for body temperature measurements," in *2014 IEEE RFID Technology and Applications Conference (RFID-TA)*, 2014.

[33] S. Amendola, G. Bovesecchi, P. Coppa, and G. Marrocco, "Thermal characterization of epidermal RFID sensor for skin temperature measurements," in *2016 IEEE International Symposium on Antennas and Propagation (APSURSI)*, 2016.

[34] R. Colella and L. Catarinucci, "Wearable UHF RFID sensor tag in 3D-printing technology for body temperature monitoring," in *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*, 2018.

[35] W. Zhu, Q. Zhang, M. Matlin, Y. Chen, Y. Wu, X. Zhu, H. Zhao, R. Pollack, and H. Xiao, "Passive digital sensing method and its implementation on passive RFID temperature sensors," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 4793–4800, Nov 2020.

[36] Farsens, "EPC C1G2 Compliant UHF RFID Tag with Power Harvesting and SPI Communication for External Low Power Sensors and Actuators," Online, 2023. [Online]. Available: http://www.farsensiot.com/uploadfile/file/20210625/1624611093.pdf

[37] A. Beriain, E. d'Entremont, J. G. de Chavarri, I. Zalbide, and R. Berenguer, "EPC C1G2 Compliant Batteryless Tire Pressure Monitoring Tag with Pressure and Tire Contact Temperature," in *Communication Technologies for Vehicles: 10th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2016, San Sebastián, Spain, June 6-7, 2016, Proceedings 10*. Springer, 2016, pp. 163–172.

[38] A. Vena, B. Sorli, B. Saggin, R. Garcia, and J. Podlecki, "Passive UHF RFID sensor to monitor fragile objects during transportation," in *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*. IEEE, 2019, pp. 415–420.

[39] Powercast. (2023) Datasheet for: PCT100/PCT200 Sensor Tag. https://www.powercastco.com/wp-content/uploads/2021/06/PCT100-PCT200-V2.1-ONE-PAGE.pdf. Powercast® High-Function RFID Sensor Tags.

[40] Powercast—. (2023) Datasheet for: TX91501B/TX91503 Sensor Tag. https://www.powercastco.com/wp-content/uploads/2021/06/PCT100-PCT200-V2.1-ONE-PAGE.pdf. Powercast® High-Function RFID Sensor Tags.

[41] Wiliot. (2023) Wiliot Platform: IoT Pixels. https://www.wiliot.com/product/iot-pixels.

[42] Confidex. (2024) Confidex Heatwave Tough ŤM Datasheet RFID Tag. [Online]. Available: https://rfid.atlasrfidstore.com/hubfs/1_Tech_Spec_Sheets/Confidex/ATLAS%20Confidex%20Heatwave%20ToughTM%20RFID%20Tag%20Data%20Sheet.pdf?_gl=1*cpgruj*_ga*MTc3NTIzMjc4Ni4xNzA4MDE4Mzc5*_ga_27CW97GZK8*MTcxMDc5MjQ0Ni4zLjAuMTcxMDc5MjQ0Ni42MC4wLjA.

[43] *STEVAL-PROTEUS Data Brief: Industrial Sensor Evaluation Kit for Condition Monitoring Based on the 2.4 GHz STM32WB5MMG Module*, STMicroelectronics, 2023. [Online]. Available: https://www.st.com/en/evaluation-tools/steval-proteus1.html

[44] E. Pantoja, R. Sreekumar, S. Mosanu, T. Tracy, and M. Stan, "Virtualized Controller for Computational RFID-based IoT Sensors," in *2023 IEEE International Conference on RFID (RFID)*. IEEE, 2023, pp. 54–59.

[45] Landaluce *et al.*, "A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks," *Sensors*, vol. 20, no. 9, p. 2495, 2020.

[46] Liu *et al.*, "Fast RFID Sensory Data Collection: Trade-off Between Computation and Communication Costs," *IEEE/ACM Transactions on Networking*, vol. 27, no. 3, pp. 1179–1191, 2019.

[47] Chen *et al.*, "CRFID: An RFID System with a Cloud Database as a Back-end Server," *Future Generation Computer Systems*, vol. 30, pp. 155–161, 2014.

[48] Yeager *et al.*, "WISP: A Passively Powered UHF RFID Tag with Sensing and Computation," in *RFID Handbook*. CRC Press, 2017, pp. 261–276.

[49] K. Ding and P. Jiang, "RFID-Based Production Data Analysis in an IoT-Enabled Smart Job-Shop," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 128–138, 2017.

[50] Xue *et al.*, "Edge Computing for Internet of Things: A Survey," in *International Conferences on Internet of Things*. IEEE, 2020, pp. 755–760.

[51] Zhong *et al.*, "RFID-Enabled Real-Time Advanced Planning and Scheduling Shell for Production Decision Making," *International Journal of Computer Integrated Manufacturing*, vol. 26, no. 7, pp. 649–662, 2013.

[52] R. Horne and J. C. Batchelor, "A Framework for a Low Power On Body Real-Time Sensor System Using UHF RFID," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 4, pp. 391–397, 2020.

[53] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient RF Energy-Harvesting Technologies for Self-Sustainable Standalone Wireless Sensor Platforms," *Proceedings of the IEEE*, vol. 102, no. 11, pp. 1649–1666, 2014.

[54] Zeadally *et al.*, "Design Architectures for Energy Harvesting in the Internet of Things," *Renewable and Sustainable Energy Reviews*, vol. 128, p. 109901, 2020.

[55] G. R. Espinosa, B. Montrucchio, E. Giusto, and M. Rebaudengo, "Low-cost PM Sensor Behaviour Based on Duty-Cycle Analysis," in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2021, pp. 1–8.

[56] Y. Cai, S. M. Reddy, I. Pomeranz, and B. M. Al-Hashimi, "Battery-aware dynamic voltage scaling in multiprocessor embedded system," in *2005 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2005, pp. 616–619.

[57] J. Yin and M. R. Stan, "A low power SRAM with fully dynamic leakage suppression for IoT nodes," in *2023 24th International Symposium on Quality Electronic Design (ISQED)*, 2023, pp. 1–8.

[58] EM Microelectronic. (2023) 18000-63 type c (gen2) and 18000-63 type c/18000-64 type d (gen2/total) RFID IC. [Online]. Available: https://www.emmicroelectronic.com/product/epc-and-uhf-ics/em4325

[59] Analog Devices. (2023) Micropower 3-axis digital output MEMS accel ADXL362. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/ADXL362.pdf

[60] I. Amihai, R. Gitzel, A. M. Kotriwala, D. Pareschi, S. Subbiah, and G. Sosale, "An industrial case study using vibration data and machine learning to predict asset health," in *2018 IEEE 20th Conference on Business Informatics (CBI)*, vol. 1. IEEE, 2018, pp. 178–185.

[61] D. Catenazzo, B. O'Flynn, and M. Walsh, "On the use of wireless sensor networks in preventative maintenance for Industry 4.0," in *2018 12th International Conference on Sensing Technology (ICST)*. IEEE, 2018, pp. 256–262.

[62] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram, S. Raza *et al.*, "Fog computing: An overview of big IoT data analytics," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[63] L. AlAwlaqi, A. AlDawod, R. AlFowzan, and L. AlBraheem, "The Requirements of Fog/Edge Computing-Based IoT Architecture," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2021, pp. 0051–0057.

[64] J. Chen and X. Ran, "Deep learning with edge computing: A review," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1655–1674, 2019.

[65] F. Zhou, Y. Wu, R. Q. Hu, and Y. Qian, "Computation rate maximization in UAV-enabled wireless-powered mobile-edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1927–1941, 2018.

[66] E. Pantoja, R. Sreekumar, S. Mosanu, T. Tracy, and M. Stan, "Virtualized controller for computational RFID-based IoT sensors," in *2023 IEEE International Conference on RFID (RFID)*. IEEE, 2023, pp. 54–59.

[67] F.-T. Zohra, O. Salim, S. Dey, H. Masoumi, and N. Karmakar, "Machine Learning Approach to RFID Enabled Health Monitoring of Coal Mine Conveyor Belt," *IEEE Journal of Radio Frequency Identification*, 2023.

[68] C. Occhiuzzi, F. Camera, M. D'Orazio, N. D'Uva, S. Amendola, G. M. Bianco, C. Miozzi, L. Garavaglia, E. Martinelli, and G. Marrocco, "Automatic monitoring of fruit ripening rooms by UHF RFID sensor network and machine learning," *IEEE Journal of Radio Frequency Identification*, vol. 6, pp. 649–659, 2022.

[69] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[70] RFID4U, " RFID Basics - EPC Gen2 Memory," https://rfid4u.com/rfid-epc-gen2-memory/, 2024, accessed: 2024-03-22.

[71] GS1, "EPC UHF Gen2 Air Interface Protocol," https://www.gs1.org/standards/rfid/uhf-air-interface-protocol, 2024, accessed: 2024-03-22.

[72] S. M. Noghabaei, R. L. Radin, Y. Savaria, and M. Sawan, "A high-efficiency ultra-low-power CMOS rectifier for RF energy harvesting applications," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2018, pp. 1–4.

[73] J. Kang, P. Chiang, and A. Natarajan, "Bootstrapped rectifier–antenna co-integration for increased sensitivity in wirelessly-powered sensors," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 11, pp. 5031–5041, 2018.

[74] Z. Wu, Y. Zhao, Y. Sun, H. Min, and N. Yan, "A self-bias rectifier with 27.6% pce at-30dbm for rf energy harvesting," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2021, pp. 1–5.

[75] S. M. Noghabaei, R. L. Radin, Y. Savaria, and M. Sawan, "A high-efficiency ultra-low-power CMOS rectifier for RF energy harvesting applications," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018, pp. 1–4.

[76] Z. Wu, Y. Zhao, Y. Sun, H. Min, and N. Yan, "A self-bias rectifier with 27.6% PCE at -30dBm for RF energy harvesting," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021, pp. 1–5.

[77] S. Pellerano, J. Alvarado, and Y. Palaskas, "A mm-wave power harvesting RFID tag in 90nm CMOS," in *2009 IEEE Custom Integrated Circuits Conference*, 2009, pp. 677–680.

[78] A. Mohan and S. Mondal, "An impedance matching strategy for micro-scale RF energy harvesting systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 4, pp. 1458–1462, 2021.

[79] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "Co-design of a CMOS rectifier and small loop antenna for highly sensitive RF energy harvesters," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 3, pp. 622–634, 2014.

[80] K. Kotani, A. Sasaki, and T. Ito, "High-efficiency differential-drive CMOS rectifier for UHF RFIDs," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 11, pp. 3011–3018, 2009.

[81] M. A. Al-Absi, I. M. Alkhalifa, A. A. Mohammed, and A. A. Al-Khulaifi, "A CMOS rectifier employing body biasing scheme for RF energy harvesting," *IEEE Access*, vol. 9, pp. 105 606–105 611, 2021.

[82] B. Nikolić, M. Blagojević, O. Thomas, P. Flatresse, and A. Vladimirescu, "Circuit design in nanoscale FDSOI technologies," in *2014 29th International Conference on Microelectronics Proceedings - MIEL 2014*, 2014, pp. 3–6.

[83] T. S. Ho, H. Ramiah, K. K. P. Churchill, Y. Chen, C. C. Lim, N. S. Lai, P.-I. Mak, and R. P. Martins, "Low voltage switched-capacitive-based reconfigurable charge pumps for energy harvesting systems: An overview," *IEEE Access*, vol. 10, pp. 126 910–126 930, 2022.

[84] R. Rao, N. DasGupta, and A. DasGupta, "Study of random dopant fluctuation effects in FD-SOI MOSFET using analytical threshold voltage model," *IEEE Transactions on Device and Materials Reliability*, vol. 10, no. 2, pp. 247–253, 2010.

[85] W. C. Bartra, A. Vladimirescu, and R. Reis, "Process and temperature impact on single-event transients in 28nm FDSOI CMOS," in *2017 IEEE 8th Latin American Symposium on Circuits & Systems (LASCAS)*. IEEE, 2017, pp. 1–4.

[86] W. X. Lian, H. Ramiah, G. Chong, and K. K. P.C, "A differential RF front-end CMOS transformer matching for ambient RF energy harvesting systems," in *2021 IEEE Asia Pacific Conference on Circuit and Systems (APCCAS)*, 2021, pp. 133–136.

[87] E. Pantoja and M. Stan, "Advancing Wireless IoT Sensor Networks With Edge-Powered RFID Devices," in *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2023, pp. 0632–0636.

[88] A. Khattab, Z. Jeddi, E. Amini, M. Bayoumi, A. Khattab, Z. Jeddi, E. Amini, and M. Bayoumi, "RFID security threats and basic solutions," *RFID Security: A Lightweight Paradigm*, pp. 27–41, 2017.

[89] M. Hutter, T. Plos, and M. Feldhofer, "On the security of RFID devices against implementation attacks," *International Journal of Security and Networks*, vol. 5, no. 2-3, pp. 106–118, 2010.

[90] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, "Maximalist cryptography and computation on the WISP UHF RFID tag," *Wirelessly Powered Sensor Networks and Computational RFID*, pp. 175–187, 2013.

[91] C. Pendl, M. Pelnar, and M. Hutter, "Elliptic curve cryptography on the WISP UHF RFID tag," in *RFID. Security and Privacy: 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers 7*. Springer, 2012, pp. 32–47.

[92] A. Szekely, M. Höfler, R. Stögbuchner, and M. Aigner, "Security enhanced wisps: Implementation challenges," *Wirelessly Powered Sensor Networks and Computational RFID*, pp. 189–204, 2013.

[93] M. Hamann, "Lightweight cryptography on ultra-constrained RFID devices," *Universität Mannheim*, 2018.

[94] A. Kumar, S. Jain, and A. Aggarwal, "Comparative Analysis of Multi-round Cryptographic Primitives based Lightweight Authentication Protocols for RFID-Sensor Integrated MANETs." *Journal of Information Assurance & Security*, vol. 14, no. 1, 2019.

[95] A. Arbit, Y. Livne, Y. Oren, and A. Wool, "Implementing public-key cryptography on passive RFID tags is practical," *International Journal of Information Security*, vol. 14, no. 1, pp. 85–99, 2015.

[96] R. Chatterjee and R. Chakraborty, "A modified lightweight PRESENT cipher for IoT security," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*. IEEE, 2020, pp. 1–6.

[97] T.-N. Lam, D.-H. Le *et al.*, "Implementation of Lightweight Cryptography Core PRESENT and DM-PRESENT on FPGA," in *2022 International Conference on Advanced Technologies for Communications (ATC)*. IEEE, 2022, pp. 104–109.