SASYR Symposium of Applied Science for Young Researchers

3rd Symposium of Applied Science for Young Researchers

PROCEEDINGS 2023

July 11, 2023

3rd Symposium of Applied Science for Young Researchers

Proceedings

SASYR 2023

11 July 2023

Editors

Florbela P. Fernandes
Research Centre in Digitalization and Intelligent Robotics (CeDRI)
Instituto Politécnico de Bragança

Pedro Morais
Applied Artificial Intelligence Laboratory (2Ai)
Instituto Politécnico do Cávado e do Ave

Pedro Pinto
Applied Digital Transformation Laboratory (ADiT-LAB)
Instituto Politécnico de Viana do Castelo

Instituto Politécnico de Bragança — 2023
Campus de Santa Apolónia
5300-253 Bragança – Portugal
ISBN: 978-972-745-324-5

Book cover: Natália Santos, Instituto Politécnico do Cávado e do Ave

Welcome

This document presents the proceedings of the 3rd Symposium of Applied Science for Young Researchers - SASYR. This scientific event welcomed works by junior researchers on any research topic covered by the following three research centers: ADiT-lab (from IPVC, Instituto Politécnico de Viana do Castelo), 2Ai (from IPCA, Instituto Politécnico do Cávado e do Ave) and CeDRI (from IPB, Instituto Politécnico de Bragança). The main objective of SASYR is to provide a friendly and relaxed environment for young researchers to present their work, discuss recent results, and develop new ideas. In this way, this event offered an opportunity for the ADiT-lab, 2Ai, and CeDRI research communities to gather synergies and promote collaborations, thus improving the quality of their research. The SASYR 2023 took place at Instituto Politécnico do Cávado e do Ave, Barcelos, Portugal, on the 11th of July, 2023.

The SASYR 2023 Organizing Committee,
Florbela P. Fernandes
Pedro Morais
Pedro Pinto

Committees

Organizing Committee

Florbela P. Fernandes, CeDRI, Instituto Politécnico de Bragança
Pedro Morais, 2Ai, Instituto Politécnico do Cávado e do Ave
Pedro Pinto, ADiT-lab, Instituto Politécnico de Viana do Castelo

Advisory Committee

Ana Pereira, CeDRI, Instituto Politécnico de Bragança
José Lima, CeDRI, Instituto Politécnico de Bragança
Paulo Leitão, CeDRI, Instituto Politécnico de Bragança
João L. Vilaça, 2Ai, Instituto Politécnico do Cávado e Ave
António Miguel Cruz, ADiT-lab, Instituto Politécnico de Viana do Castelo
Jorge Garcia, ADiT-lab, Instituto Politécnico de Viana do Castelo

Technical Support

Carla Fontes, Instituto Politécnico de Bragança
Clarisse Pais, Instituto Politécnico de Bragança
Pedro Oliveira, Instituto Politécnico de Bragança
Susana Carvalho, Instituto Politécnico do Cávado e do Ave
Silvestre Malta, Instituto Politécnico de Viana do Castelo

Scientific Committee

Alberto Simões, 2Ai, Instituto Politécnico do Cávado e do Ave
Ana Isabel Pereira, CeDRI, Instituto Poliécnico de Bragança
André Mendes, CeDRI, Instituto Poliécnico de Bragança
Andreia Teixeira, ADiT-lab, Instituto Politécnico de Viana do Castelo
Ângela Ferreira, CeDRI, Instituto Poliécnico de Bragança
Ângela Silva, ADiT-lab, Instituto Politécnico de Viana do Castelo
António Cruz, ADiT-lab, Instituto Politécnico de Viana do Castelo
Antonio Moreira, 2Ai, Instituto Politécnico do Cávado e do Ave
Carla Soares Geraldes, CeDRI, Instituto Poliécnico de Bragança
Carlos Abreu, ADiT-lab, Instituto Politécnico de Viana do Castelo
Cátia Alves, 2Ai, Instituto Politécnico do Cávado e do Ave
Clara Vaz, CeDRI, Instituto Poliécnico de Bragança
Daniel Miranda, 2Ai, Instituto Politécnico do Cávado e do Ave
Diogo Lopes, 2Ai, Instituto Politécnico do Cávado e do Ave
Duarte Duque, 2Ai, Instituto Politécnico do Cávado e do Ave
Estela Vilhena, 2Ai, Instituto Politécnico do Cávado e do Ave

Eva Oliveira, 2Ai, Instituto Politécnico do Cávado e do Ave
Fernando Monteiro, CeDRI, Instituto Poliécnico de Bragança
Florbela P. Fernandes, CeDRI, Instituto Poliécnico de Bragança
João Carlos Silva, 2Ai, Instituto Politécnico do Cávado e do Ave
João L. Vilaça, 2Ai, Instituto Politécnico do Cávado e do Ave
João Paulo Coelho, Instituto Poliécnico de Bragança
João Paulo Teixeira, CeDRI, Instituto Poliécnico de Bragança
Joaquim Gonçalves, 2Ai, Instituto Politécnico do Cávado e do Ave
Jorge Ribeiro, ADiT-lab, Instituto Politécnico de Viana do Castelo
Jose Henrique Brito, 2Ai, Instituto Politécnico do Cávado e do Ave
José Lima, CeDRI, Instituto Poliécnico de Bragança
Jose Rufino, CeDRI, Instituto Poliécnico de Bragança
Luis Ferreira, 2Ai, Instituto Politécnico do Cávado e do Ave
Luís Teófilo, ADiT-lab, Instituto Politécnico de Viana do Castelo
Luisa Jorge, CeDRI, Instituto Poliécnico de Bragança
Manuela Cruz-Cunha, 2Ai, Instituto Politécnico do Cávado e do Ave
Maria F. Pacheco, CeDRI, Instituto Poliécnico de Bragança
Maria Mourão, ADiT-lab, Instituto Politécnico de Viana do Castelo
Natália Rego, 2Ai, Instituto Politécnico do Cávado e do Ave
Nuno Lopes, 2Ai, Instituto Politécnico do Cávado e do Ave
Óscar Ribeiro, 2Ai, Instituto Politécnico do Cávado e do Ave
Patrícia Leite, 2Ai, Instituto Politécnico do Cávado e do Ave
Paula Alexandra Rego, ADiT-lab, Instituto Politécnico de Viana do Castelo
Paulo Costa, ADiT-lab, Instituto Politécnico de Viana do Castelo
Paulo Leitao, CeDRI, Instituto Poliécnico de Bragança
Paulo Matos, CeDRI, Instituto Poliécnico de Bragança
Pedro Morais, 2Ai, Instituto Politécnico do Cávado e do Ave
Pedro Pinto, ADiT-lab, Instituto Politécnico de Viana do Castelo
Pedro Rodrigues, CeDRI, Instituto Poliécnico de Bragança
Rui Pedro Lopes, CeDRI, Instituto Poliécnico de Bragança
Sara Paiva, ADiT-lab, Instituto Politécnico de Viana do Castelo
Sérgio Lopes, ADiT-lab, Instituto Politécnico de Viana do Castelo
Teresa Abreu, 2Ai, Instituto Politécnico do Cávado e do Ave
Tiago Pedrosa, CeDRI, Instituto Poliécnico de Bragança
Vítor Carvalho, 2Ai, Instituto Politécnico do Cávado e do Ave

Table of Contents

Feeding Digital Soil Twins with data collected from an IoT sensor network

Letícia Silva[1,3], João Paulo Coelho[1,4], Francisco J. Rodríguez-Sedano[3], and Paula C. Baptista[2,4]

[1] Research Center for Digitization and Intelligent Robotics (CeDRI),Campus de Santa Apolónia, 5300-253 Bragança, Portugal
leticiadasilva, jpcoelho }@ipb.pt
[2] Mountain Research Center (CIMO), Polytechnic Institute of Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
pbaptista@ipb.pt
[3] Robotics Group, Engineering School, University of León, Campus de Vegazana s/n, 24071 León, Spain
[4] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

Abstract. Digital twins have great potential to promote productivity and improve product quality. However, in the agricultural context, this paradigm has exhibited slow penetration due to several limitations such as process complexity, heterogeneity, and dynamic conditions, among many others. One of the research lines of the MAN4HEALTH project aims to promote the integration of digital twins into olive groves. In this frame of reference, the digital twin's state space must be populated with different types of Information; some are provided manually by the user and others are retrieved automatically from sensor nodes scattered along the field. This paper describes the sensor network implemented for the project in which details regarding the adopted methodology and IoT technologies are documented.

Keywords: Smart Agriculture · Soil Digital Twin · Predictive Control.

1 Introduction

This paper addresses the implementation of a sensor network and IoT technologies for the integration of digital twins in olive groves, in which, the potential of digital twins in promoting productivity and improving soil quality, in the agricultural sector, is underlined. However, it also recognizes the challenges in this context, such as the complexity of the process, the heterogeneity, and the dynamic soil conditions.

The MAN4HEALTH project aims to integrate intelligent techniques, the Internet of Things, and soil management techniques, in olive groves. A sensor network was implemented, which, consists of IoT sensor nodes distributed throughout the production area, collecting data on soil parameters through various sensors. The collected data is used to feed the digital twin-state space, enabling real-time monitoring and predictive control. In addition, providing the information for making informed decisions, on soil management practices and optimizing olive production.

In summary, the paper characterizes the implementation of an IoT sensor network and its integration with digital twins in agriculture, demonstrating the potential to improve productivity and optimize soil management practices in olive groves.

2 Related Works

Digital Twins (DT) emerged in the early 2000s by M. Grieves [1], although many authors credit NASA (National Aeronautics and Space Administration of the United States of America). Grieves and Vickers worked together to adapt the concept of DT in manufacturing to improve product lifecycle management [1, 2]. At their most basic level, DTs can be seen as realistic virtual representations of entities with physical or logical existence, such as machines or processes [3].

Extrapolation from industry to sectors such as agriculture is a natural step since the same goals of increasing productivity and controlling product quality are typical concerns. Therefore, the virtualisation of agriculture emerges as an answer, as there is a directly proportional relationship between productivity and digitalisation [4, 5].

However, despite this potential, its use in this context is still at an early stage of implementation [6, 7]. There are several reasons why the use of DT in agriculture has not yet made a substantial leap forward. Thus, agricultural processes are usually more complex than industrial processes, presenting heterogeneous and dynamic conditions, requiring spatial and temporal data resolutions that may not be technically and economically feasible [3].

DTs are still being defined and it appears that the benefits of their use are particularly expressive in cases where normal asset management and control systems are of limited utility. Examples of DTs that successfully and seamlessly combine these elements in a complex operational environment are rare or non-existent [8].

The slow penetration of DT in agricultural processes is due to current limitations, such as the low amount of technical resources, lack of communication means in remote farms, scarcity of economic resources, continuous climate change, soil quality, and low technical qualification of agricultural producers [9]. Despite the existence of a history of using DT in smart farming applications, it is still an evolving field.

3 Project Man4Health

In Portugal, the soil of olive groves is subject to severe degradation due to harsh farming techniques and uncontrollable weather conditions that cause serious problems in this region specifically. The MAN4HEALTH project proposes a multidisciplinary solution that correlates the potential of two research centres, the Centre for Mountain Research (CIMO) and the Centre for Digitalization and Intelligent Robotics Research (CeDRI). The project aims to find a suitable mix of indigenous plants that can be used as cover crops to improve soil quality, together with the addition of smart farm management techniques.

For this purpose, a set of experiments has been planned in an olive grove located near Mirandela, a town situated in north-eastern Portugal. The whole plot, which has a total area of about 3.8 ha, for the purpose of the different trials, was divided into eight distinct zones, as shown in Figure 1. In the figure, 24 square areas are shown. Which, each square, with has a total area of 49 m^2, equivalent to a total of four olive trees. As can be observed in the figure, each black circles indicated represent the trees, mentioned.

During the trials, the soil area referred to as the red bottom squares was treated with tillage procedures. The soil area referring to the upper squares, in green, was subjected to mechanical seeding procedures. In addition, for each of these plots, regular sampling was performed to assess the evolution of soil quality. This procedure was carried out on a scheduled basis and each sample was evaluated for its microbial content and mechanical characteristics.

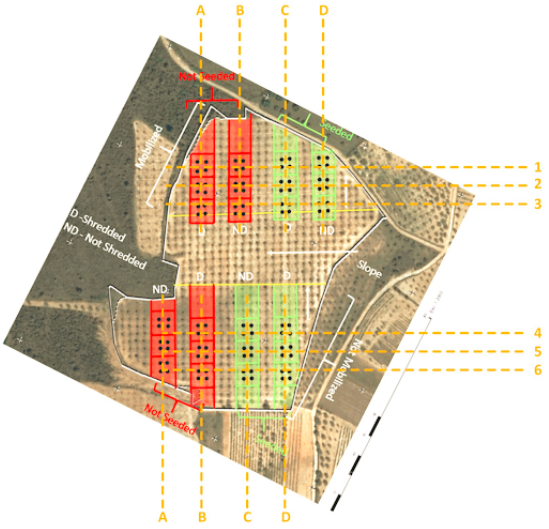


Fig. 1: Top view of the sensor network in Olive Grove.

4 Proposed Cyber-Physical System: Digital Twin

In the following section, you will present in detail the Sensor Node Network.

4.1 Sensor Node Network

A network of IoT (Internet of Things) sensor nodes has been designed and installed, in an olive grove in north-eastern Portugal. These finished nodes are customized and will be distributed along the production area, to automatically collect data about several physicochemical parameters of the soil.

Which, each IoT measurement node have to collect local information about the meteorological characteristics of the soil, such as moisture, electroconductivity, pH, and temperature of the soil. Data collection is relevant to estimate the true state of soil nutrition. Since the nutritional requirements of the olive trees can have significant spatial variability, the data will be acquired by geographical sampling over the whole production area, using the mentioned measurement nodes.

In this way, the nodes play an important role in supporting the status information to be used by a Soil Digital Twin (DT). The data generated by the customised set made by the measurement nodes will be transmitted to a remote centre, in which, the

DT performs the processing and predictive control. For this purpose, each node will be equipped with a LoRa based transceiver which will be responsible for sending the measurements to a LoRa concentrator (gateway) [10, 11]. Two different types of nodes have been developed, the solar panel node and the battery powered IoT node, and will be presented in Figure 2.

The first, the Solar Panel node, is capable of measuring parameters such as soil temperature and moisture, pH, and electroconductivity. This node has been sized and installed, has an off-grid power system and the configuration includes a lead/gel battery with a capacity of 65 Ah, an MPPT solar charge regulator, and a 285 W polycrystalline solar panel with 60 cells. This node is fixed on the ground by means of a support structure (pole), which contains the electrical panel and the solar panel. On top of the galvanised steel pole are located, the LTE Dragino gateway (DLOS8 LoRa), a Hydreon rain sensor, an external surveillance camera (IP67), and a SenseCAP ORCH S4 4-in-1 weather station.

The developed system will be responsible for the task of providing the necessary power to a local processing unit, constituted by a single board computer. This, acts as a bridge between the various types of existing communication protocols. This way, the access to the internal states of the MPPT charge controller and the weather station is made through the Modbus protocol, which works through RS485. Data from all these devices is sent by the SBC to the LoRa gateway through an IEEE 802.11 (WiFi) wireless communication protocol. The solar panel node is shown in Figure 2.

Finally, for the battery node, the power supply consists of a 3.7 V, 2600 mAh Li-ion battery, and a 3.3 V DC-DC voltage regulator. The regulated voltage will power the LoRa transceiver, which in the current configuration was the RFM95. The analog and digital signals provided by the set of sensors connected to this module are fed to the microcontroller (ATMega328). For this reason, and together with firmware and hardware design choices, the average hourly consumption of the measured nodes is about 590 µA. Given this value, and according to the battery charge value, each node is expected to be able to operate for a time interval of 180 days (without being recharged).

Each measurement node is designed for low power consumption and is powered by a lithium-ion battery that provides one year of longevity between charges. Data is sent, via the LoRa portal, to a FIWARE stack responsible for context management. The information from all these measuring points is aggregated in a hub, in this case a LoRa gateway, which will be responsible for transmitting the data to the context agent via a 4G/LTE backhaul connection.

These sensors have the ability to measure different properties of soil (moisture at different depths, temperatures), air (moisture at different depths, temperatures), light intensity, and battery charge. The autonomous node is shown in Figure 2.

5 Data and Soil Model

Regarding the data model, the context entities and all the information associated with the current system will be managed by a platform based on FIWARE, developed for the implementation of IoT applications and open source. All context information, collected and managed by FIWARE, will be available for the DT model.

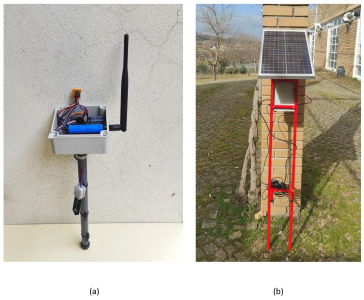


Fig. 2: Node representation diagram. (a) Autonomous Node. (b) Solar Panel Node

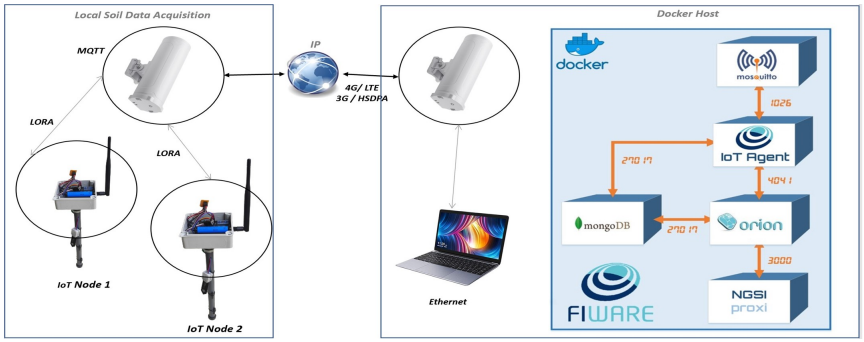


Fig. 3: Overview of the data architecture in the IoT sensor network

FIWARE is an open-source initiative that defines a universal set of standards for context data management. The concept of context and the definition of the architecture of this platform are based on the information model known as NGSI-LD. All these entities are instantiated in FIWARE's Orion broker which, in addition to context management, provides an API that can be used to query and retrieve data.

The data connection between each custom IoT node and the gateway will be managed by a LoRa-based protocol. Each JSON-based payload packet transmitted by the measurement nodes to the gateway will be sent to an MQTT broker using a 3G/4G mobile communication infrastructure. From a logical point of view, each node will be an entity whose context information and temporal persistence are managed by a broker running on a system based on the FIWARE ecosystem [12]. Figure 3 represents the described the overview of the data architecture in the IoT sensor network.

Therefore, the proposed system will address the digital soil twin (DT), as a virtual model of soil dynamics. All the developed intelligent nodes will collect information about the soil state in real-time. This set of inputs will be analysed together with other external contextual data and integrated into the digital twin. Due to soil heterogeneity, global soil models will be addressed through a spatial discretization where diffusion equations associated with black box models, supported by computational intelligence (machine learning) methodologies, will be used to make predictions about the actual spatial distribution of soil chemical content.

These predictions, together with the vegetative state of olive production, will be used in a model-based predictive control methodology. In this paradigm, the best soil practices, such as the concentration of fertilizer to apply in a given area, will be calculated based on the long and short-term predictions provided by the digital twin. The objective function that will shape the behaviour of the controller will take into account the impact of current soil management policies on soil health, overall olive yield, and farmer profit [13, 14].

Figure 4, represents the proposed system, called DT. In the physical environment is the olive grove, where the network of sensors that collect soil and environmental parameters is being installed. In the digital environment, the data collected are managed by FIWARE, which is sent to the soil model. From the modeled data, and the parameters received from the weather forecast and from the farmer, Machine Learning is used. The results of this are sent to the farmer, making it possible to make long and short-term forecasts about the best olive grove management practices. The Farmer controls the actuator, in order to manage the agricultural production in the olive grove.

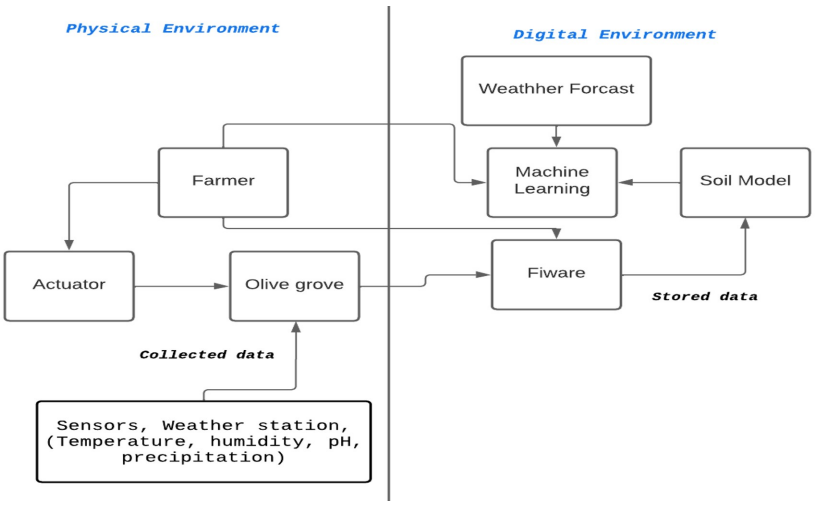


Fig. 4: Digital Soil Twin Representation.

6 Conclusion

Digital twins (DTs) are virtual representations of physical objects, processes or systems that are increasingly being adopted in factories to improve productivity and product lifecycle management.

The data generated by the customized set made by the measurement nodes will be transmitted to a remote central, in which, the DT performs processing and predictive control. For this purpose, each node will be equipped with a LoRa-based transceiver that will be responsible for sending the meters to a LoRa concentrator (gateway). It is expected that in the future, this sensor network will be able to feed the digital terrestrial twin with the collected data.

The developed nodes will play an important role in supporting the state information that will be used by a Digital Soil Twin (DT). The sensor network will provide data to the soil DT, which can be used to predict soil conditions and recommend optimal management practices to improve the productivity and quality of agricultural products.

With the digital representation of the dynamics that soil undergoes as a result of different policies and management options, it is intended to make long-term predictions regarding the evolution of its quality. Ultimately, it is expected that the knowledge of trends in the evolution of soil characteristics, together with a predictive control strategy, will lead to a regulation of soil characteristics towards optimal operating conditions.

Acknowledgment

This work was supported by NORTE 2020—FEDER funds, within the project "Man4Health—New management strategies in olive groves for improving soil health and crop yield", NORTE-01-0145- FEDER-000060". The authors are also grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021).

References

1. Cor Verdouw, Bedir Tekinerdogan, Adrie Beulens, and Sjaak Wolfert. Digital twins in smart farming. *Agricultural Systems*, 189:103046, 2021.
2. Abozar Nasirahmadi and Oliver Hensel. Toward the next generation of digitalization in agriculture based on digital twin paradigm. *Sensors*, 22(2):498, 2022.
3. Fei Tao, Jiangfeng Cheng, Qinglin Qi, Meng Zhang, He Zhang, and Fangyuan Sui. Digital twin-driven product design, manufacturing and service with big data. *The International Journal of Advanced Manufacturing Technology*, 94:3563–3576, 2018.
4. Klaus Schwab. *The fourth industrial revolution*. Currency, 2017.
5. Leonello Trivelli, Andrea Apicella, Filippo Chiarello, Roberto Rana, Gualtiero Fantoni, and Angela Tarabella. From precision agriculture to industry 4.0: Unveiling technological connections in the agrifood sector. *British Food Journal*, 121(8):1730–1743, 2019.
6. Bedir Tekinerdogan and Cor Verdouw. Systems architecture design pattern catalog for developing digital twins. *Sensors*, 20(18):5103, 2020.
7. Mats Söderström, Gustav Sohlenius, Lars Rodhe, and Kristin Piikki. Adaptation of regional digital soil mapping for precision agriculture. *Precision Agriculture*, 17:588–607, 2016.
8. Melanie Jans-Singh, Kathryn Leeming, Ruchi Choudhary, and Mark Girolami. Digital twin of an urban-integrated hydroponic farm. *Data-Centric Engineering*, 1:e20, 2020.
9. TR Sreedevi and MB Santosh Kumar. Digital twin in smart farming: A categorical literature review and exploring possibilities in hydroponics. *2020 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*, pages 120–124, 2020.
10. Antonio Valente, Carlos Costa, Leonor Pereira, Bruno Soares, José Lima, and Salviano Soares. A lorawan iot system for smart agriculture for vine water status determination. *Agriculture*, 12(10):1695, 2022.
11. Ancha Srinivasan. *Handbook of precision agriculture: principles and applications*. CRC press, 2006.
12. JA López-Riquelme, N Pavón-Pulido, H Navarro-Hellín, F Soto-Valles, and R Torres-Sánchez. A software architecture based on fiware cloud for precision agriculture. *Agricultural water management*, 183:123–135, 2017.
13. Gopal Chaudhary, Manju Khari, and Mohamed Elhoseny. *Digital Twin Technology*. CRC Press, 2021.
14. Ismael da Silva Pena. Arquitetura de controle para gestão de recursos na agricultura de precisão. 2019.

Speaker Recognition in Door Access Control System

Enrico Manfron[1,3], João Paulo Teixeira[1,2], and Rodrigo Minetto[3]

[1] Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
enricomanfron@alunos.utfpr.edu.br, joaopt@ipb.pt
[3] Federal University of Technology – Paraná, 80230-901 Curitiba, Brazil
rminetto@utfpr.edu.br

Abstract. In this paper, we explore the potential of speaker recognition technology as a biometric authentication method for access control systems. We focus on the development and evaluation of two machine learning models, the Gaussian Mixture Model (GMM) and Multilayer Perceptron (MLP), for speaker identification. Our research presents a review of speaker recognition literature, followed by a detailed methodology for constructing and training the GMM and MLP models on a specific dataset. Experimental results highlight the performance of these models in terms of accuracy and efficiency. This study contributes to the application of GMM and MLP models for speaker recognition-based access control systems, serving as a resource for future research and development in secure and effective access control solutions.

Keywords: Speaker recognition · Gaussian Mixture Model (GMM) · MLP (Multilayer Perceptron).

1 Introduction

Speaker recognition is a technology with potential applications in biometric authentication, which can be employed in access control systems for secure environments. In recent years, progress has been made in speaker recognition technology, including the development of sophisticated algorithms and machine learning models. By analyzing the unique characteristics of an individual's voice, this technology can accurately identify people and grant them access to restricted areas.

This paper presents the initial work on the development and evaluation of two speaker recognition models: the Gaussian Mixture Model (GMM) and the Multilayer Perceptron (MLP). We begin with a review of the literature on speaker recognition, followed by a detailed description of the methodology employed to develop the GMM and MLP models, as well as the dataset used for training and testing. Finally, we present and analyze the experimental results obtained from the evaluation of both models.

This paper contributes by developing and evaluating two machine learning models. Our objective is to present our initial work on speaker recognition-based access control systems by exploring the application of GMM and MLP models. Our research describes how we build and train these models and present the experimental results we obtained. We believe that this work can serve as a resource for future research in this area, as well as aid in the development of more secure and efficient access control systems.

2 Related Work

In recent years, the field of speaker recognition (SR) has seen significant advancements, driven by the development of novel techniques and the growing availability of large datasets. As a result, a significant number of research articles have been published to explore various aspects of SR, from fundamental concepts and methodologies to the latest state-of-the-art models.

Among these early approaches, Gaussian Mixture Models (GMM) emerged as a popular and powerful technique in the pre-deep learning era of SR, from 1995 to 2006. The GMMs models were applied in numerous applications in computer vision, speech recognition, and speaker recognition, thanks to their ability to approximate complex distributions using a combination of simple Gaussian distributions [1]. Deep learning has been the dominant machine learning approach since around 2010 [2].

The concept shares similarities with Gaussian mixture models, using simple functions called neurons to approximate complex functions. In speech signal processing, recurrent neural networks have been particularly useful due to their ability to model sequence data effectively [3]. Deep learning models are more scalable and efficient when handling large datasets, with specialized hardware like GPUs and TPUs available for acceleration. From 2014 onwards, the field of speaker recognition has seen numerous advancements in deep learning models.

Hanifa et al. [2] provides a comprehensive survey of SR models, addressing major issues such as background noise, lack of data, and attacks on models. It presents a chronology of the field's development, highlighting the technologies created and the progress made. Researchers have explored various preprocessing techniques, common features extracted in the field, potential model types and classifiers, and application areas.

Examples include a 2010 study that employed 3 Discrete Wavelet Transform (DWT) with different coefficients, using a Multilayer Perceptron (MLP) and a Gaussian Mixture Model (GMM) as classifiers [4]. Both models achieved high accuracy (98% and 99%), but the MLP could be trained with audio samples half the duration of those used in the GMM model. In subsequent years, research utilized neural networks, such as the Fuzzy Min-Max Neural Network (FMMNN) [5], as well as variations of the GMM model [6], and comparisons with Hidden Markov Model (HMM), all using Mel Frequency Cepstral Coefficients (MFCC) vectors as input [7].

Later attempts explored variations of MFCC features, such as Normalized Dynamic Spectral Features (NDSFs) and Linear Prediction Cepstral Coefficients (LPCCs), to determine if these sets could provide better feature representation than MFCCs [8]. The field then shifted to using convolutional neural networks [9] and x-vectors for their robustness to noise [10]. Recent studies in the survey employed combinations of the aforementioned features, such as MFCCs + PNCC [11] and LDA + MFCCs [12], among others.

3 Methodology and Results

In this research, we developed a methodology to explore and understand Speaker Recognition (SR) techniques through the implementation of early SR approaches, including the Gaussian Mixture Model (GMM), GMM-UBM, and the Multilayer Perceptron (MLP) model. These implementations allowed us to compare different approaches in the SR domain and develop a deeper understanding of the underlying concepts and challenges.

For the GMM implementation, we began by extracting the first 20 MFCCs from each audio file, consisting of 32 speakers. This resulted in a matrix $m \times n$, where m is related to the audio duration and n is equal to 20, as we are using the first 20 MFCCs.

We created 32 GMM models, one for each speaker, and extracted the 20 MFCCs from each audio file. We concatenated the tables with the MFCCs for each speaker and divided the data into 80% for training and 20% for testing. A GMM model with 32 Gaussians was trained for each speaker. After training, we used a function that calculates the average log-likelihood per sample of the provided data. To identify a speaker, we took a speech sample and compared it to all GMM models, selecting the model with the highest score as the most probable representation of the speaker.

In this first approach, the model correctly recognized all speakers in the test set; however, since the GMM model assumes a closed set, it attempts to identify the speaker from the set by assigning a score to the most likely candidate. This makes it impossible to determine the presence of an imposter that is out of the set. Following this method, when processing an imposter's speech, we would have a score for each model, and the imposter would be classified with the model with the lowest score, incorrectly assigning the imposter instead of rejecting them.

This initial GMM model is a Speaker Identification model, where the task is to identify which speaker said a given phrase. However, we are now interested in verifying if a speech came from a specific speaker, which is called Speaker Verification.

To perform Speaker Verification (i.e., to determine if the speaker is who they claim to be), another approach called the Universal Background Model (UBM) is necessary [13]. This approach uses a speaker-independent GMM model to represent alternative speakers or imposters. We then reduce the problem to test two hypotheses:

H_0: The utterance is from the hypothetical speaker S.

H_1: The utterance is not from the hypothetical speaker S.

To calculate the model, we use the log-likelihood ratio, defined as:

$$L(X) = \ln p(X|H_0) - \ln p(X|H_1) \tag{1}$$

Where X is the feature vector extracted from the speech utterance.If $L(X) \geq 0$, we accept Hypothesis H_0; otherwise, we accept Hypothesis H_1.

To implement the above-described approach, two methods were applied. In the first method, for a single speaker S, a GMM model containing only S's training data and a GMM-UBM model containing data from all speakers excluding S were trained. In total, there were 32 GMM models and 32 GMM-UBM models for each speaker, resulting in two GMM models for each speaker. In this approach, the model recognized 30 out of the 32 speakers, however, the 2 unrecognized speakers' scores were really near zero.

We test a new approach based on the proposal of Reynolds [13], where the idea for creating the GMM-UBM is slightly different. First, we used all the training data to create the GMM-UBM. Then, using an algorithm called Bayesian Adaptation, the UBM model was adapted for each speaker's specific data. In the end, there were 32 GMMs, one for each speaker, and a single UBM. Although it is possible to re-adapt the weights, means, and covariances, the best approach is to adapt only the means. The training pipeline is illustrated in Figure 1.

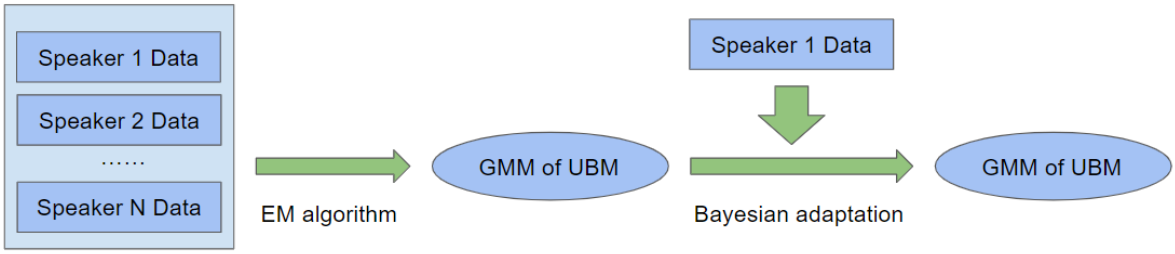


Fig. 1: GMM-UBM training pipeline using Bayesian Adaptation algorithm.

After training, there was a slight improvement in the number of correct identifications, now the model accepts 31 out of 32 speakers. However, the system using this approach resulted in more false positives.

Based on the work done by Kral et al. [4], our study focuses on implementing a Multilayer Perceptron (MLP) model for speaker recognition. We build upon the existing research that demonstrates the effectiveness of MFCCs in speaker recognition tasks.

For the initial testing phase, Model A, a simple Multilayer Perceptron (MLP) model was created to classify 32 speakers. The architecture of all MLP models is shown in Table 1. The model took the first 13 MFCCs, delta MFCCs, and delta-delta MFCCs as input features for a descriptor size of 39 features. The MLP architecture consisted of three hidden layers with 256, 128, and 64 neurons, respectively. The audio features were efficiently extracted and saved in a CSV file, allowing for easier feature selection. The initial tests achieved an accuracy of 74% using CrossEntropy as the loss function, training for 50 epochs, in Figure 2 it is shown the loss function during the training.

Table 1: MPL architecture.

Layer (type)	Input Shape	Output Shape
Linear-1	N	256
Linear-3	256	128
Linear-5	128	64
Linear-7	64	32

Subsequently, the model could be trained for mode epochs and an early stopping mechanism was implemented in order to optimize time training. This attempt, which utilized the same MLP architecture for classification, will be referred to as Model B for

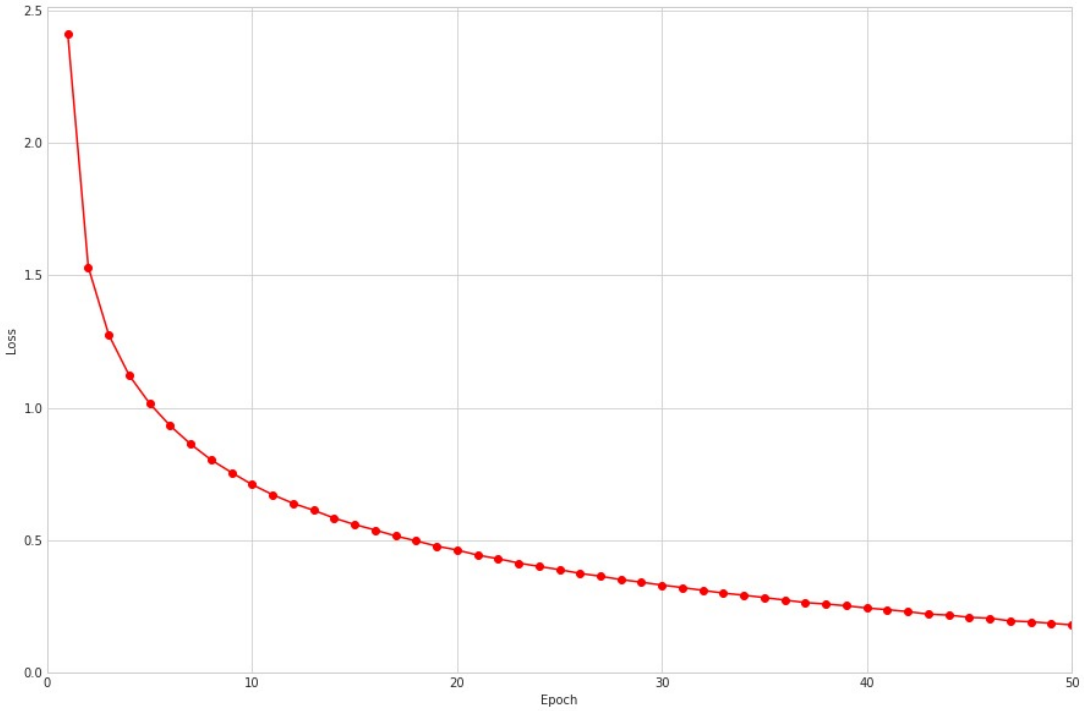


Fig. 2: Train Loss function for MLP model for 50 epochs.

future reference. Model B was used for classification with 70% of the data allocated for training, 10% for validation (early stopping), and 20% for testing. The early stopping criteria were initially based on the loss function but later switched to accuracy, as it was observed that accuracy could still improve even when the loss increased.

The highest accuracy achieved with this model was 91.12% on the test data. It was hypothesized that the increasing loss with improved accuracy might be due to class imbalance caused by varying audio lengths among speakers, which results in different numbers of MFCCs vectors extracted per speaker.

Additional features were incorporated into the model, which we will refer to as Model C, such as chroma stft, rmse, spectral centroid, spectral bandwidth, spectral roll-off, zero crossing rate, and more MFCCs (20 columns) for a total descriptor with size of 77 features. The input size increased, and the model was trained over 500 epochs. This resulted in a validation accuracy of 93.48% and a test accuracy of 92.19%. The training became more stable with the increased number of features, although the loss still increased.

Finally, the learning rate was reduced from 0.001 to 0.0001, leading to more stable training and a further improvement in accuracy. The model, which we will refer to as Model D, achieved 93.4% validation accuracy and 93.33% test accuracy.

The loss and accuracy during the training could be seen in Figure 3.

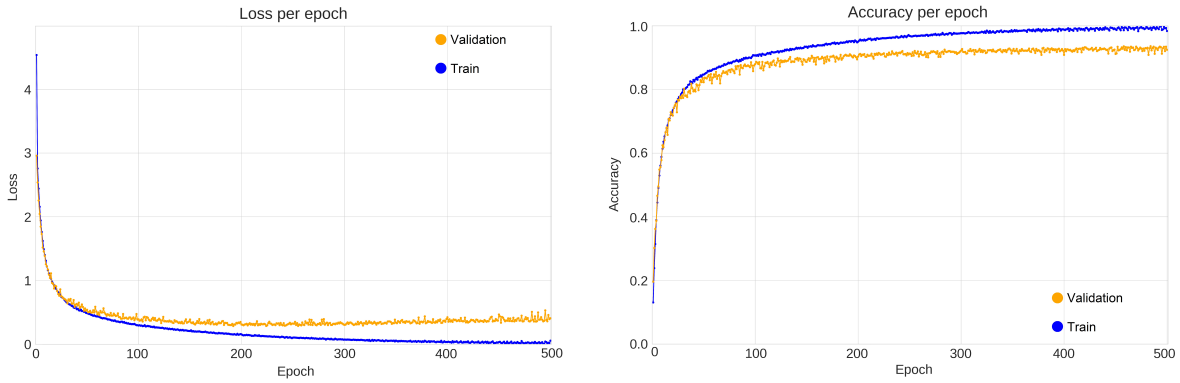


Fig. 3: Train Loss and Accuracy function for MLP model for 500 epochs.

A comparison of the MLP network's results can be found in Table 2.

Table 2: Performance of MLP Model Across Attempts

model	Input Features	Validation Accuracy	Test Accuracy
Model A	MFCC(13), ΔMFCC(13), Δ^2MFCC(13)	–	0.74
Model B	MFCC(13), ΔMFCC(13), Δ^2MFCC(13)	0.9176	0.9112
Model C	MFCC(20), ΔMFCC(20), Δ^2MFCC(20), chroma stft(12), rmse(1), spectral centroid(1), spectral bandwidth(1), spectral rolloff(1), zero crossing rate(1)	0.9348	0.9219
Model D	MFCC(20), ΔMFCC(20), Δ^2MFCC(20), chroma stft(12), rmse(1), spectral centroid(1), spectral bandwidth(1), spectral rolloff(1), zero crossing rate(1)	0.934	0.9333

4 Conclusion

This study demonstrates the effectiveness of a Multi-Layer Perceptron (MLP) model for speaker identification using various audio features. The integration of additional features has all contributed to a more robust and accurate model.

The results show that an MLP model can achieve high accuracy in speaker classification, with the best model reaching 93.33% on test data. These findings highlight the importance of using a diverse set of features and optimizing hyperparameters, such as the learning rate, to achieve better performance. By decreasing the learning rate value, the model showed more stable behavior, enabling a slow and steady adjustment of the neural network weights throughout training. This resulted in a better convergence of the training process. In the end, these modifications allowed the model to learn better and find a superior solution, which improved its performance on the given task.

Despite the promising results, there are still some challenges that need to be addressed. The increase in the loss during training, probably due to class imbalance,

warrants further investigation to improve the model's stability and generalization. Future work could explore techniques such as data augmentation, resampling, or other mechanisms to handle class imbalance more effectively.

Additionally, other architectures, such as Transformer Networks Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs), could be considered for speaker classification tasks to evaluate their performance in comparison to the MLP model. Exploring recent deep-learning models for speaker recognition presents a way for future work. We are already in the process of developing and evaluating such models, aiming to build better models for this task further.

In summary, this paper presents a foundation for further research and development in speaker classification using neural networks. The results achieved by the MLP model in this study demonstrate its potential for real-world applications, while the challenges identified provide valuable insights for future improvements.

Acknowledgments

The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021).

References

1. D.A. Reynolds and R.C. Rose. Robust text-independent speaker identification using gaussian mixture speaker models. *IEEE Transactions on Speech and Audio Processing*, 3:72–83, 1995.
2. Rafizah Mohd Hanifa, Khalid Isa, and Shamsul Mohamad. A review on speaker recognition: Technology and challenges. *Computers & Electrical Engineering*, 90:107005, 2021.
3. Takaaki Hori, Jaejin Cho, and Shinji Watanabe. End-to-end speech recognition with word-based rnn language models. In *2018 IEEE Spoken Language Technology Workshop (SLT)*. IEEE, 2018.
4. Pavel Kral. Discrete wavelet transform for automatic speaker recognition. In *2010 3rd International Congress on Image and Signal Processing*. IEEE, 2010.
5. N. P. Jawarkar, R. S. Holambe, and T. K. Basu. Use of fuzzy min-max neural network for speaker identification. In *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*. IEEE, 2011.
6. P. Krishnamoorthy, H.S. Jayanna, and S.R.M. Prasanna. Speaker recognition under limited data condition by noise addition. *Expert Systems with Applications*, 38(10):13487–13490, 2011.
7. Hesham Tolba. A high-performance text-independent speaker identification of arabic speakers using a CHMM-based approach. *Alexandria Engineering Journal*, 50(1):43–47, 2011.
8. Sharada V. Chougule and Mahesh S Chavan. Robust spectral features for automatic speaker recognition in mismatch condition. *Procedia Computer Science*, 58:272–279, 2015.
9. Joon Son Chung, Arsha Nagrani, and Andrew Zisserman. VoxCeleb2: Deep speaker recognition. In *Interspeech 2018*. ISCA, 2018.
10. Jesús Villalba, Nanxin Chen, David Snyder, Daniel Garcia-Romero, Alan McCree, Gregory Sell, Jonas Borgstrom, Fred Richardson, Suwon Shon, François Grondin, Réda Dehak, Leibny Paola García-Perera, Daniel Povey, Pedro A. Torres-Carrasquillo, Sanjeev Khudanpur, and Najim Dehak. State-of-the-art speaker recognition for telephone and video speech: The JHU-MIT submission for NIST SRE18. In *Interspeech 2019*. ISCA, 2019.
11. Bharath K P and Rajesh Kumar M. ELM speaker identification for limited dataset using multitaper based MFCC and PNCC features with fusion score. *Multimedia Tools and Applications*, 79:28859–28883, 2020.
12. K.Y Zergat, S.A. Selouani, and A. Amrouche. Feature selection applied to g.729 synthesized speech for automatic speaker recognition. In *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*. IEEE, 2018.

13. Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. Speaker verification using adapted gaussian mixture models. *Digital Signal Processing*, 10(1-3):19–41, 2000.

Machine Learning Methods Applied to Predictive Maintenance: a Literature Review

Matheus Pinto[1], Arthur Bertachi[3], and Ana I. Pereira[1,2]

[1] Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Bragança, Portugal
a57019@alunos.ipb.pt, apereira@ipb.pt
[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[3] Federal University of Technology - Paraná (UTFPR), Guarapuava, Brazil
abertachi@utfpr.edu.br

Abstract. Predictive has become an essential tool for the industry, as it allows for the identification of component failures before they even occur, reducing unplanned interruptions and increasing process efficiency and productivity. With the advancement of technology, especially in Industry 4.0, data collection has become even more common, making machine learning methods a promising and necessary tool for processing the large amount of data and achieving greater accuracy in fault identification. However, the proper selection of a machine learning method is a determining factor for the success of the process. This work presents a literature review of machine learning methods applied to predictive maintenance, showing which techniques are being explored in this approach, how they are being applied, and which equipment predictive maintenance is being employed on.

Keywords: Predictive maintenance · Machine learning · Literature review.

1 Introduction

The growing pursuit of efficiency and productivity through the development of artificial intelligence technologies has made predictive maintenance an increasingly required strategy in Industry 4.0 [1]. This approach consists of collecting and analyzing data to predict failures in components and systems even before they occur, allowing for preventive repairs and replacements at the most optimized moment possible, reducing downtime and repair costs [2].

To harness the benefits of predictive maintenance, the utilization of advanced technologies such as the Internet of Things (IoT) and Big Data has become instrumental. These technologies enable the acquisition of large volumes of sensor and equipment data, which can be further analyzed to detect anomalies and identify patterns that may signify an impending failure [1]. Given the complexity and scale of this data, machine learning methods have emerged as an essential tool to effectively interpret and extract valuable insights from it, enabling accurate failure predictions and optimized maintenance processes [3].

For predictive maintenance, various methods are explored to leverage machine learning and increase the effectiveness of maintenance operations. These methods encompass a wide range of techniques, including supervised learning and reinforcement learning. Supervised learning algorithms such as Support Vector Machines (SVM) and Random

Forests (RF) have been widely adopted to build predictive models using labeled training data [4], which is the focus of this article. Additionally, reinforcement learning techniques have started to gain attention for their ability to learn good maintenance policies through interactions with the environment [5].

In addition to the various machine learning methods, the type of equipment and systems undergoing predictive maintenance is equally significant. Predictive maintenance techniques have been successfully applied in many domains, including factories, power generation facilities, transportation systems, and more. In manufacturing, for example, critical assets such as turbines, engines and pumps are closely monitored to detect signs of degradation or possible failures [6]. Likewise, in power generation plants, predictive maintenance plays a vital role in ensuring the reliable operation of turbines, generators and transformers [7]. Transportation systems such as railroads and airlines depend on predictive maintenance to increase safety and optimize maintenance schedules for components such as engines, brakes and signaling systems [8, 9].

In this sense, this article aims to provide support for the understanding and improvement of the use of machine learning in predictive maintenance. To this end, a literature review will be conducted to address the methods used in this area, the origin of the data sets used, and the equipment that undergoes these analyses. The goal of this research is to contribute to the improvement of the efficiency of the algorithms applied in predictive maintenance through a more in-depth understanding of the use of machine learning in this context.

The structure of this article is organized as follows: Section 2 presents the literature review, addressing the planning protocols and execution of the review. Section 3 discusses the results of the literature review. Finally, Section 4 concludes the article and suggests ideas for future work.

2 Literature Review

Literature review is a widely used method in scientific research to evaluate information related to a specific topic. Its purpose is to allow the researcher to understand what has already been studied on the topic, identify gaps in knowledge, and possible directions for future research [10].

The literature review has several advantages, such as rigorous evaluation of study quality, extraction of essential information, and consolidation of relevant findings. To be well executed, it is necessary to be comprehensive and critical, which implies seeking different sources of information, evaluating the quality of these sources, verifying the credibility of the authors, analyzing the methodology used, and its relevance to the proposed topic [10].

To conduct a literature review, it is necessary to follow some steps, such as precisely defining the research questions, conducting a thorough literature search, and establishing selection criteria, among other procedures. It is important that these steps are conducted rigorously and with attention to ensure the quality and reliability of the literature review [11].

In order to ensure the quality of the research, the PRISMA methodology is adopted as the basis for the literature review. This tool is used to ensure that information is

presented clearly and objectively, enabling other researchers to evaluate and replicate the research results [12]. The choice of the PRISMA methodology as the basis for the review is due to its wide use in the scientific community and the existence of a published study in the area that will serve as a parameter for comparison with the review conducted in this article [4, 13].

2.1 Literature Review Process

The starting point of this review consists of defining the research questions, since it is these questions that guide the research objectives, defining its purpose and ensuring that all relevant aspects are considered. Therefore, the research questions that guide this study are:

- Q_1. How is Machine Learning applied in Predictive maintenance?
- Q_2. What are the Machine Learning methods used to predict the Remaining Useful Life of equipment?
- Q_3. On which equipment are these methods applied?
- Q_4. What are the dataset used?
- Q_5. Are the data used real or synthetic?

To continue this study, it is necessary to define the literature sources that will be researched. In this sense, for this study, three widely recognized scientific databases were chosen: IEEEXplore[4], Scopus[5], and Web of Science[6].

In addition, at this stage of the research, the selection parameters of the studies are established, which define the inclusion and exclusion criteria to be adopted. For this study, the exclusion criteria are:

- E_1. Publications published in more than one database
- E_2. Publications that do not pertain to Predictive Maintenance and Machine Learning.
- E_3. Publications that do not present results related to Remaining Useful Life.
- E_4. Publications that do not present any comparison means.

After excluding the documents that do not meet the established criteria, the relevant characteristics that will be individually analyzed in each selected article are enumerated. These characteristics will be used as the basis for the discussion of the obtained results, ensuring a rigorous and reliable evaluation of the study. This process of selecting and analyzing articles aims to guarantee the accuracy and objectivity of the presented results. The data extraction fields are:

- D_1. Year of publication.
- D_2. Machine learning method used.
- D_3. Equipment, case, or scenario in which the Predictive Maintenance techniques were applied
- D_4. Origin of the data, whether it was synthetic or real data.

[4] ieeexplore.ieee.org
[5] scopus.com
[6] webofscience.com

2.2 Execution

The selection of keywords to conduct the bibliographic search was based on a previous study [4], which used the expressions 'machine learning' and 'predictive maintenance', both in their full and abbreviated forms. As there was a significant increase in interest in the topic, it was decided to add a third keyword to limit and direct the search towards the proposed objective, namely, the term 'remaining useful life'.

The Remaining Useful Life (RUL) metric is widely used in predictive maintenance, along with the concept of 'time to failure', to estimate the time until a product or equipment failure. Based on this, the keywords and their abbreviated forms are presented in Table 1 below:

Table 1: Keywords searched

Full form	**Abbreviated form/Synonym**
Predictive maintenance	PdM
Machine learning	Artificial intelligence
Remaining useful life	RUL

Consequently, search strings were elaborated for each of the selected databases, as described below:

- **IEEEXplore**: ("predictive maintenance" OR "PdM") AND ("machine learning" or "artificial intelligence") AND ("RUL" or "remaining useful life")
- **Scopus**: TITLE-ABS-KEY (("predictive maintenance" OR "PdM") AND ("machine learning" OR "artificial intelligence") AND ("RUL" OR "remaining useful life"))
- **Web of Science**: ALL = (("predictive maintenance" OR "PdM") AND ("machine learning" or "artificial intelligence") AND ("RUL" or "remaining useful life"))

Table 2: Lists the main nomenclature used in this paper.

Abbreviation	**Definition**
ANN	Artificial Neural Network
DT	Decision Tree
k-NN	k-Nearest Neighbors
LR	Linear Regression
NB	Naive Bayes
RD	Real Data
RF	Random Forests
SD	Synthetic Data
SVM	Support Vector Machine
SVR	Support Vector Regression

3 Results and Discussion

The research was conducted in March 2023, with the application of a temporal limit filter, restricting the search to documents published between 2018 and the present moment (2018-2023). A total of 355 documents were identified, out of which 148 were duplicates, i.e., were included in more than one database. After applying all the established exclusion criteria, 12 articles were selected for the present review.

Fig. 1 shows the number of articles resulting from the removal of duplicates, published between January 2018 and March 2023, accompanied by a trend line. The review confirms that the use of machine learning techniques in predictive maintenance for remaining useful life prediction is a new approach, since only one article had been published on the subject in 2018. However, after this period, there was a significant increase in related studies, with an average of just over 20 articles per year in 2018-2020, and over 48 articles on average in the years 2021-2023 (taking into account that the research was conducted in March 2023, leaving the remainder of the year to be counted). This fact may be related to the dissemination of artificial intelligence studies as a means of productivity gain.

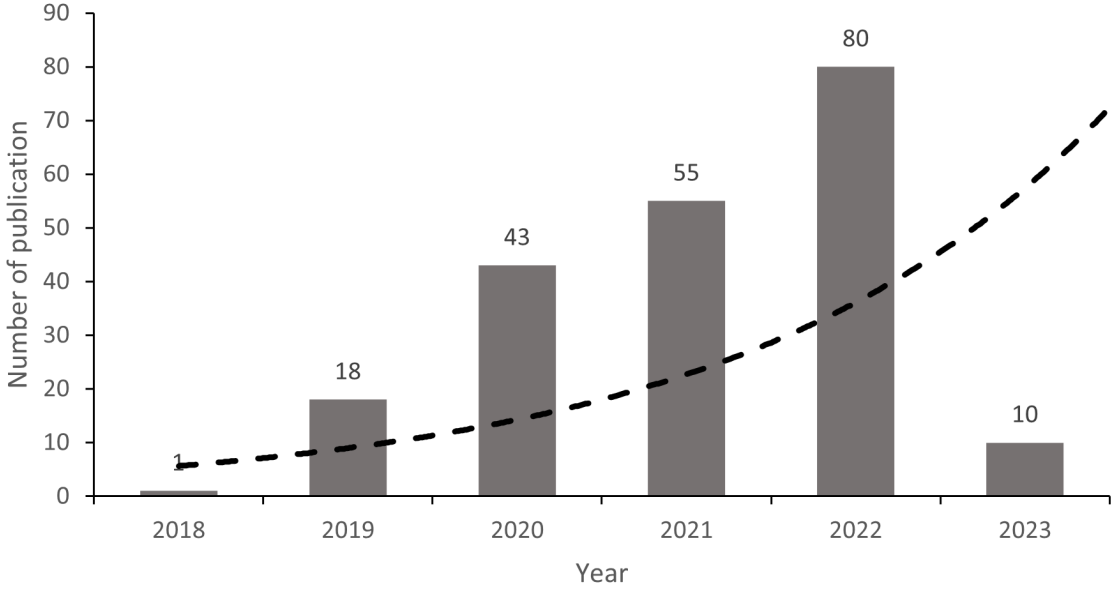


Fig. 1: Number of papers per year with a trend line from 2018

After the completion of the review, a summary of the analysis of the selected articles is provided, from which significant conclusions can be drawn. This information is displayed in a summarized form in Table 3, whose nomenclature is presented in Table 2.

By conducting a comparative analysis with the study published in [4], it is possible to observe a wide variety of equipment used in predictive maintenance, especially when

Table 3: Summary of the selected publications on predictive maintenance.

Reference	ML method(s)	Case	Data type
[6]	SVR, ANN	Aircraft engine	SD
[14]	ANN, SVM	Bearings in grinding machines	RD
[15]	ANN	Aircraft engine	SD
[16]	k-NN, NB , RF, SVM	BLDC motor	RD
[8]	ANN	Wheel-bearing component of a railcar	RD
[17]	LR	Aircraft engine	SD
[7]	SVM, ANN	Wind turbine shaft bearings	RD
[9]	LR, DT, SVM, RF, k-NN, ANN	Aircraft engine	SD
[18]	ANN	Aircraft engine	SD
[19]	SVM	Aircraft engine	SD
[20]	LR, ANN, DT, RF	Aircraft engine	SD
[21]	RF	Rolling Bearings	RD

it comes to real sensor data, which represents 89% of the selected articles. However, in this study, it is observed that this type of data represents less than half of the analyzed documents. It is therefore concluded that researchers have given preference to synthetic data for performing remaining useful life prediction. Furthermore, the part that represents synthetic data belongs to a single dataset, which provides high credibility in the academic field.

As mentioned earlier, the equipment derived from synthetic data refers to a single device. On the other hand, the remaining equipment is related to various sectors and plays a vital role in those areas, such as factories, power generation, and transportation systems. However, they are applied to small mechanical components within complex structures [7]. This approach can be explained by the fact that we are in the early stages of studying predictive maintenance using machine learning [4]. As this technique evolves, there is the possibility of applying it to larger equipment.

Regarding the machine learning methods employed, there is no consensus, since various algorithms are applied with their respective justifications. In addition, for the same dataset, different algorithms are used depending on the author. This fact can be exemplified by the study carried out by the authors [15], [18], and [19], who adopted different methods to predict the failure time of the same dataset.

When compared to [4], which predominantly classified random forest as the most used algorithm with a frequency of 33%, there is still no significant standout value regarding the other methods. In the present research, it was found that authors prefer to employ more than one machine learning method in their investigations, such as exemplified by the authors [16], [9], and [20], who used more than three methods for prediction.

However, it is important to highlight that the Artificial Neural Network (ANN) method had a significant representativeness, being used in eight of the twelve selected articles, both in synthetic and real data. This can be attributed to its suitability for dealing with noise from equipment sensors, recognizing hidden patterns, as described in the literature in [22]. Next, the Support Vector Machines (SVM) method appears in five documents. However, it is important to emphasize that these methods are commonly used in conjunction with others to allow for a more accurate comparative analysis.

4 Conclusions and Future Work

When analyzing the already published documents, along with the results obtained in this study, it can be observed that predictive maintenance is an innovative and effective approach for predicting failures and implementing interventions in equipment and systems. The use of machine learning techniques complements this approach and makes it viable, allowing for greater accuracy in failure prediction and increasing maintenance efficiency.

However, one limitation of this approach is the need to acquire a large volume of data to train the machine learning models. This requires a significant investment in infrastructure and technology. A viable solution to this problem is the incorporation of the IoT (Internet of Things) mentality in industries.

As a suggestion for future research, it is recommended to develop more advanced machine learning models and more consolidated validation techniques to carry out comparative studies and determine the most effective model in different scenarios.

References

1. Tiago Zonta, Cristiano André da Costa, Felipe A. Zeiser, Gabriel de Oliveira Ramos, Rafael Kunst, and Rodrigo da Rosa Righi. A predictive maintenance model for optimizing production schedule using deep neural networks. *Journal of Manufacturing Systems*, 62:450–462, 2022.
2. Niima Es-sakali, Moha Cherkaoui, Mohamed Oualid Mghazli, and Zakaria Naimi. Review of predictive maintenance algorithms applied to hvac systems. *Energy Reports*, 8:1003–1012, 2022. Technologies and Materials for Renewable Energy, Environment and Sustainability.
3. Andreas Theissler, Judith Pérez-Velázquez, Marcel Kettelgerdes, and Gordon Elger. Predictive maintenance enabled by machine learning: Use cases and challenges in the automotive industry. *Reliability Engineering & System Safety*, 215:107864, 2021.
4. Thyago P. Carvalho, Fabrízzio A. A. M. N. Soares, Roberto Vita, Roberto da P. Francisco, João P. Basto, and Symone G. S. Alcalá. A systematic literature review of machine learning methods applied to predictive maintenance. *Computers & Industrial Engineering*, 137:106024, 2019.
5. Jing Huang, Qing Chang, and Jorge Arinez. Deep reinforcement learning based preventive maintenance policy for serial production lines. *Expert Systems with Applications*, 160:113701, 2020.
6. Koceila Abid, Moamar Sayed-Mouchaweh, and Laurence Cornez. Adaptive data-driven approach for the remaining useful life estimation when few historical degradation sequences are available. *Proceedings - 19th IEEE International Conference on Machine Learning and Applications, ICMLA 2020*, pages 1145–1152, 12 2020.
7. Jinsiang Shaw and Bingjie Wu. Prediction of remaining useful life of wind turbine shaft bearings using machine learning. *Journal of Marine Science and Technology*, 29:631–637, 11 2021.
8. Ilesanmi Daniyan, Khumbulani Mpofu, Rumbidzai Muvunzi, and Ikenna Damian Uchegbu. Implementation of artificial intelligence for maintenance operation in the rail industry. *Procedia CIRP*, 109:449–453, 1 2022.
9. Vimala Mathew, Tom Toby, Vikram Singh, B. Maheswara Rao, and M. Goutham Kumar. Prediction of remaining useful lifetime (rul) of turbofan engine using machine learning. *IEEE International Conference on Circuits and Systems, ICCS 2017*, 2018-January:306–311, 3 2018.
10. Claes Wohlin, Emilia Mendes, Katia Romero Felizardo, and Marcos Kalinowski. Guidelines for the search strategy to update systematic literature reviews in software engineering. *Information and Software Technology*, 127:106366, 2020.
11. Barbara Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.
12. Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M. Lalu, Tianjing Li, Elizabeth W. Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas,

Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher. The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372, 3 2021.
13. Anders Dreyer Frost, Asbjørn Hróbjartsson, and Camilla Hansen Nejstgaard. Adherence to the prisma-p 2015 reporting guideline was inadequate in systematic review protocols. *Journal of Clinical Epidemiology*, 150:179–187, 2022.
14. Sebastian Schwendemann, Zubair Amjad, and Axel Sikora. A survey of machine-learning techniques for condition monitoring and predictive maintenance of bearings in grinding machines. *Computers in Industry*, 125:103380, 2 2021.
15. Talhat Khan, Kashif Ahmad, Jebran Khan, Imran Khan, and Nasir Ahmad. An explainable regression framework for predicting remaining useful life of machines. *2022 27th International Conference on Automation and Computing: Smart Systems and Manufacturing, ICAC 2022*, 2022.
16. R. Dhaya Sree, S. Jayanthy, and E. Essaki Vigneshwaran. Estimation of remaining useful life(rul) of bldc motor using machine learning approaches. *7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings*, pages 286–291, 2022.
17. E. Saranya and P. Bagavathi Sivakumar. Data-driven prognostics for run-to-failure data employing machine learning models. *Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020*, pages 528–533, 2 2020.
18. Ziqiu Kang, Cagatay Catal, and Bedir Tekinerdogan. Remaining useful life (rul) prediction of equipment in production lines using artificial neural networks. *Sensors 2021, Vol. 21, Page 932*, 21:932, 1 2021.
19. Sara Abdelghafar, Ali Khater, Ali Wagdy, Ashraf Darwish, and Aboul Ella Hassanien. Aero engines remaining useful life prediction based on enhanced adaptive guided differential evolution. *Evolutionary Intelligence*, 1:1–12, 12 2022.
20. Ozlem Ece Yurek and Derya Birant. Remaining useful life estimation for predictive maintenance using feature engineering. *Proceedings - 2019 Innovations in Intelligent Systems and Applications Conference, ASYU 2019*, 10 2019.
21. Christoph Bienefeld, Eckhard Kirchner, Andreas Vogt, and Marian Kacmar. On the importance of temporal information for remaining useful life prediction of rolling bearings using a random forest regressor. *Lubricants 2022, Vol. 10, Page 67*, 10:67, 4 2022.
22. Lei Wang, Yaru Liu, Kaixuan Gu, and Tong Wu. A radial basis function artificial neural network (rbf ann) based method for uncertain distributed force reconstruction considering signal noises and material dispersion. *Computer Methods in Applied Mechanics and Engineering*, 364:112954, 2020.

Evaluating the consumption performance of a multi agent system used to achieve comfort preferences

Pedro Filipe Oliveira[1], Paulo Novais[3], and Paulo Matos[1,3]

[1] Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
poliveira@ipb.pt, pmatos@ipb.pt
[3] Centro Algoritmi/Universidade do Minho, Departamento de Informática, Braga, Portugal
pjon@di.uminho.pt

Abstract. With this work, it was been developed a multi-agent system to manage comfort preferences, in an autonomous and completely automatic and non-invasive way for the user. Based on the use of an architecture supported by low cost hardware, namely Raspberry's, to support the different actuators present in the different spaces. To do its validation, a methodology was created to analyze consumption performance, and the results obtained in two scenarios are demonstrated, a domestic housing scenario, and a professional environment scenario. The obtained results were quite positive for the developed prototype, and validate the low cost hardware utilization.

Keywords: multi-agent · consumption · preferences.

1 Introduction

Users are increasingly looking for automatisms that make their daily lives easier. And thus allow them to have more free time for themselves, not having to worry about routine tasks. In which most of the time they are not able to optimize them in the same way, as is done by any automatic system. Still achieving autonomy, which is perhaps the characteristic most sought after by users of this type of system [1, 2].

With this work, it has been validated a multi agent system to achieve the best comfort preferences using low cost hardware like Raspberry's, and at the same time improve consumption performance. This work aims to give continuity and finalize the doctoral work presented in previous editions [3–5].

2 Materials and Methods

In this section, the different used actuators are detailed, as well the multi-agent system developed.

2.1 System Actuators

For the different actuators operation, in the different scenarios, different valences were used, and are following detailed:

Temperature/Relative Humidity

Namely in terms of heating, this was achieved through a hydraulic underfloor heating that is divided into different circuits to cover the different house areas, as well for its

control, six thermostats were used that allow in real time to send, using an API, the desired temperature. The thermostat and its operation mode, can be seen at figures 1 and 2.

Fig. 1: Thermostat desired temperature.

Fig. 2: Thermostat current temperature.

For cooling and relative humidity control, also six fan coils were used, one for each area, and controlled by individual thermostats, which also allow the desired temperature definition through an API.

Luminance/Brightness

For luminance and brightness, *Shelly* bulbs that have WIFI connection are used, that allow to control different luminance and brightness present at each individual environment, in the same way they have an API to integrate with other smart home systems, and that allow its direct control.

Sound

For sound, were used *Amazon Echo* speakers which have WIFI connection, and allow to control the sound volume and also the played music (sound source, playlist or gender) present at each individual environment, in the same way they have an API to integrate with other smart home systems, and that allow its direct control.

Security Systems

Also, was tested the possibility to use some security systems, and enable/disable this according to the user detection at the environment.

2.2 Multi-agent system architecture

The multi agent system was developed using JASON and ARGO, and the figure 3 represent the different layers architecture, to easily identify the purpose of each, and agents containing it.

There will be one principal agent who will represent local system, namely each individual environment, where it was a need to ensure individualized comfort conditions, such as a room in a house, or a office in a building. This agent will take into account any directives that may exist for this environment, such as lower or upper limits to different comfort conditions, or also safety parameters that may be critical for a given space. This agent will have a obviously prevalence relative to others, since it will be the dominant for a given environment.

With users respect, each one in the space, will also be represented by an agent, this will receive user preferences from main system, for the place where it is, as well for the time in which it is. Also in this situation there will be a prioritization that

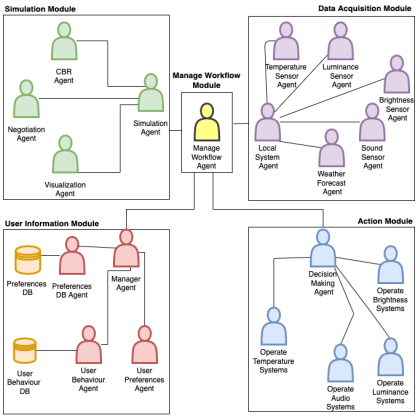


Fig. 3: Multi-agent system architecture

identifies which user will have environment supremacy, so it also has an increase in the negotiation process.

In decision-making process, all users agents and agents representing the environment will be taken into account. With the different priorities that each of them has, and with this information will begin the negotiation process.

2.3 Evaluation scenarios

For the proposed framework analysis and evaluation, different scenarios were formulated. Initially it was applied in a two floors house.

In this way, it was possible to validate the domestic space concept, with a family composed of two adult users and a child, characterized before.

Their individual preferences were defined, and the MAS system analysis was carried out during a six months period. The workspace concept was also defined, with different local systems being installed in the partner company's offices.

In section 3 the two defined scenarios results, are detailed, and explained for each of the aspects analyzed.

Home Scenario

Table 1 characterizes the different users that compose the home scenario.

Username	Type	Proportion
User1	Adult	1
User2	Adult	1
User3	Child	0,75

Table 1: Home Scenario - Users characterization.

All the entry records (samples) considered for analysis are represented, and they are divided by the six months under analysis (October 2021, November 2021, December 2021, January 2022, February 2022 and March 2022).

Totalizing *15420* log records for the six months in question. Each of these samples represents one user entrance/presence, recorded by the local system. We can see an average of *84,45* samples registered for each day.

Work Scenario

Table 2 characterizes the six users that compose the work scenario.

Username	Type	Proportion
User10	Hierarchy_1	(100-1)
User20	Hierarchy_2	(100-2)
User60	Hierarchy_3	(100-3)

Table 2: Work Scenario - Users characterization.

All the entry records (samples) considered for analysis are represented, and they are divided by the six months under analysis (October 2021, November 2021, December 2021, January 2022, February 2022 and March 2022).

Totalizing *36578* log records for the six months in question. Each of these samples represents one user entrance/presence, recorded by the local system. We can see an average of *200,98* samples registered for each day.

3 Results

To assess the results, the scenarios identified in section 2.3 were defined, and implemented. Thus, a six-month period was defined for the identified scenarios analysis, as well the users present.

For the spaces characterized in section 2.3, information was then collected over a six months period. Thus, it was possible to carry out all the statistical analysis, in order to execute the results compilation presented below at section 3.1 and 3.2 and at tables 4 and 6.

As previously mentioned, the results presented are preliminary and subject to industrial secrecy by the partner company. Therefore, all possible information is presented, considering the company's intention to commercialize the developed product, there are thus several restrictions on more data availability.

3.1 Home Scenario

Regarding energy savings, and knowing that it is currently a factor that isn't and cannot be neglected by any individual user or any business entity.

Considering the costs increase with different energy types, as well the ecological footprint that its production represents, the savings metric was also calculated, always

considering that the purpose of this solution would not have this as prime factor, but indeed the maximum user comfort.

To check exact values, the month global consumption was been verified for each analyzed space, and compared with the same month global consumption, after applying the solution.

At table 3 we can see the mean value for the baseline day consumption, and the day consumption for the analyzed period, and also the difference in kWh, and the savings in percentage value. At figure 4 we can see the plot of this information.

Scenario	**Baseline Period analyzed** (kWh)	(kWh)	**Difference** (kWh)	**Savings** (%)
Home	35,2	32,05	3,15	9,84

Table 3: Home Scenario - Day Energy consumption (mean value).

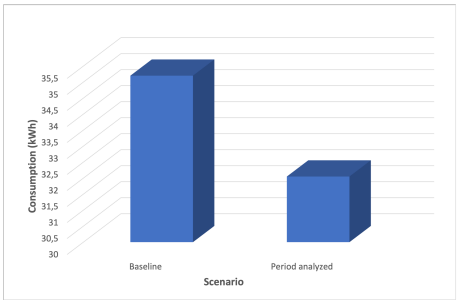


Fig. 4: Home Scenario - Day Energy consumption (mean value).

At table 4 we can see the total consumption value for the baseline, and for the 6 months period analyzed for the home scenario, and also the difference in kWh, and the savings in percentage value. At figure 5 we can see the plot of this information.

	Oct	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**	**Total**
Baseline (kWh)	806	960	1240	1426	952	930	6314
Period analyzed (kWh)	682	870	1209	1209	868	868	5706

Table 4: Home Scenario - Energy consumption - 6 Months.

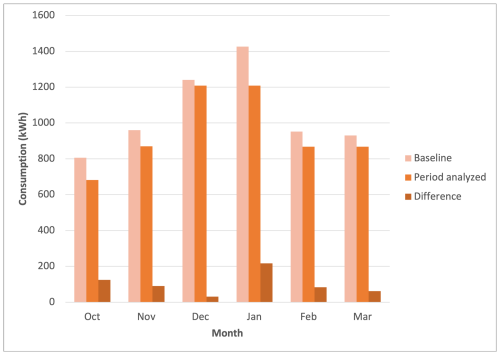


Fig. 5: Home Scenario - Energy consumption - 6 Months.

3.2 Work Scenario

At table 5 we can see the mean value for the baseline day consumption, the day consumption for the analyzed period, and also the difference in kWh, and the savings in percentage value. At figure 6 we can see the plot of this information.

Scenario	**Baseline** (kWh)	**Period analyzed** (kWh)	**Difference** (kWh)	**Savings** (%)
Work	42,5	36,4	6,1	16,76

Table 5: Work Scenario - Day Energy consumption (mean value).

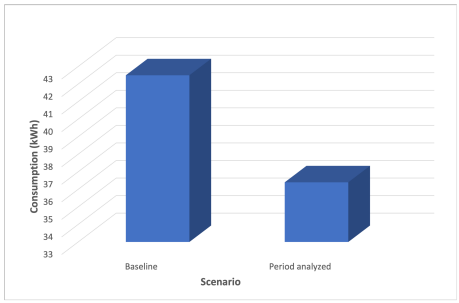


Fig. 6: Work Scenario - Day Energy consumption (mean value).

At table 6 we can see the total consumption value for the baseline, and for the 6 months period analyzed for the work scenario, and also the difference in kWh, and the savings in percentage value. At figure 7 we can see the plot of this information.

	Oct	Nov	Dec	Jan	Feb	Mar	Total
Baseline (kWh)	992	1050	1519	1643	1036	992	7232
Period analyzed (kWh)	899	840	1364	1612	868	868	6451

Table 6: Work Scenario - Energy consumption - 6 Months.

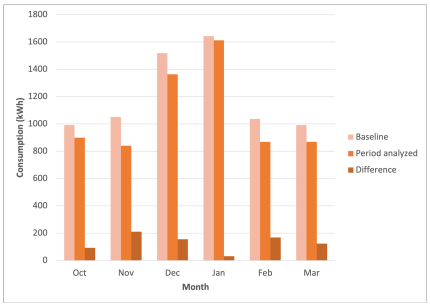


Fig. 7: Work Scenario - Energy consumption - 6 Months.

4 Conclusions

With this project, was achieved the complete development of a multi-agent system, an effective reduction in consumption.

The possibility of using low cost hardware (40€) to control this type of system was also validated. Therefore, it is effectively possible to use this type of equipment for the development of this type of project.

The 6 months analyzed period is not very extensive, but it can be seen as sufficient for this kind of spaces (domestic, small company) analysis,because users remain in some way very constant, and where there is thus no significant variance in their preferences.

Acknowledgements The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021).

References

1. Alfonso González-Briones, Pablo Chamoso, Fernando De La Prieta, Yves Demazeau, and Juan M Corchado. Agreement technologies for energy optimization at home. *Sensors*, 18(5):1633, 2018.
2. Rafael H Bordini, Jomi Fred Hübner, and Michael Wooldridge. *Programming multi-agent systems in AgentSpeak using Jason*, volume 8. John Wiley & Sons, 2007.
3. Pedro Filipe Oliveira, Paulo Novais, and Paulo Matos. A multi-agent system to manage users and spaces in a adaptive environment system. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pages 330–333. Springer, 2019.
4. Pedro Filipe Oliveira, Paulo Novais, and Paulo Matos. Using jason framework to develop a multi-agent system to manage users and spaces in an adaptive environment system. In *International Symposium on Ambient Intelligence*, pages 137–145. Springer, 2020.
5. Pedro Filipe Oliveira, Paulo Novais, and Paulo Matos. Using jason framework to develop a multi-agent system to manage users and spaces in an adaptive environment system. In *Ambient Intelligence–Software and Applications: 11th International Symposium on Ambient Intelligence*, pages 137–145. Springer, 2021.

Accuracy and Effectiveness of the Cardioban wearable medical device for monitoring Cardiovascular Health: a Critical Review.

Inês Escrivães[1,2], Diogo A. Lopes[1], Luís C. N. Barbosa[1], António H. J. Moreira[1], Vítor Carvalho[1], Leonor Varela Lema[2], João L. Vilaça[1], and Pedro Morais[1]

[1] 2AI - Applied Artificial Intelligence Laboratory - Polytechnic Institute of Cávado and Ave, Barcelos, Portugal
iescrivaes@ipca.pt

[2] Department of Preventive Medicine and Public Health, University of Santiago de Compostela, Santiago de Compostela, Spain
leonor.varela@usc.es

Abstract. The COVID-19 pandemic has made it crucial to monitor vital signs, particularly cardiovascular signals, for maintaining good health and preventing future problems. Wearable medical devices have become increasingly popular for real-time monitoring of cardiovascular health. The Cardioban, developed by Plux Biosignals, is a promising device to provide insights into a user's cardiovascular health and detect early warning signs of heart disease. To evaluate its accuracy and effectiveness we conducted a critical review by comparing its readings with those of a certified clinical device and evaluated its ability to detect early warning signs of heart disease. This review is crucial for ensuring the accuracy of wearable medical devices and ultimately the safety and well-being of patients, and it can give healthcare providers and patients confidence in the accuracy of these devices.
We processed the data obtained from both the Cardioban and the clinical device used in a hospital environment to enable a direct comparison between the two devices. We used statistical techniques, including Ttest, Peak count, Bland-Altman, as well as matching the waves when normalized to a single wavelength. Our study found that the Cardioban device performs comparably well to the regulated clinical machine used in our study, suggesting its potential as a viable alternative for cardiovascular monitoring.

Keywords: Wearable medical devices · Cardiovascular health monitoring · Vital signs · Accuracy assessment · Remote patient monitoring.

1 Introduction

Wearable medical devices have gained popularity in recent years due to their ability to monitor health in real time and provide valuable data for individuals, healthcare providers, and researchers [1]. These devices can range from simple fitness trackers that monitor steps and calories burned to sophisticated devices that track vital signs such as heart rate, blood pressure, and oxygen saturation [2]. Wearable devices are increasingly being used for the management and prevention of various health conditions, including cardiovascular disease, respiratory disorders, and diabetes [3]. The use of wearable devices has been shown to improve patient outcomes, reduce healthcare costs, and enhance the quality of care [4]. However, the accuracy and effectiveness of these devices can vary, and it is important to evaluate their performance to ensure that they are safe and reliable for medical use. In particular, the accuracy of devices that monitor

cardiovascular health is critical, as early detection and treatment of cardiovascular diseases can significantly reduce the risk of complications and improve the overall quality of life [5], [6].

2 The Wearable Medical Device: CardioBan

The cardioban (Fig. 1) is a wearable device that uses multiple sensors to collect data on heart rate, heart rate variability, respiratory rate, skin temperature, and physical activity levels.Is a non-invasive wearable device that utilizes a singlelead ECG signal to detect various cardiovascular parameters. It is worn around the chest, and the data is transmitted wirelessly to a smartphone app, where it can be analyzed and interpreted. This data is then processed using the signals coming from the sensors and the device displays metrics to the user, allowing for the evaluation of their health status.

Fig. 1: Various views of the Cardioban. This wearable medical device was developed by Plux Biosignals, Lda.

3 Methodology

The study was conducted at the 2Ai - Laboratory of Applied Artificial Intelligence, in the School of Technology, Polytechnic Institute of Cavado and Ave (IPCA). The purpose of the study was to compare the reliability and confidence of the CardioBan device, developed by PLUX Biosignals, with the GE Vivid E9 ultrasound machine, which is used for regulated hospital use. The study was designed to collect data from the cardiac signal of participants using both devices, with the aim of evaluating the accuracy of the CardioBan device. Data was collected from participants over 18 years of age who were conscious and aware of their motor and psychic activities, and had given their consent. The data obtained from the two devices was processed and analyzed using statistical techniques such as the T-test, Peak count, Bland-Altman analysis, and Normalization.

4 Results

In order to provide a detailed examination of the results at the individual level, a randomly selected participant's data will be presented visually (Figs. 2 and 3). As part of my ongoing efforts to streamline and focus the content of my paper were decided to

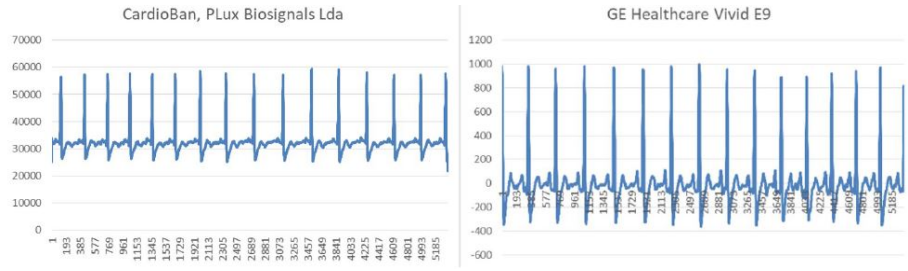


Fig. 2: ECG signal from the two devices used in the study. On the left, the Cardioban ECG signal, and on the right, the ECG signal from the GE Healthcare Vivid E9 regulated clinical machine.

restrict the discussion to just two of the analytical tests that were performed (namely peak counting and normalization).

Regarding the quantification of peaks in two ECG signals obtained from a single participant but recorded using two distinct monitoring devices. Figure 2 indicates that the two signals are highly similar. The maximum discrepancy between the two signals is noted to be two peaks. This observation suggests that both devices effectively capture the same ECG signal with consistent periodicity and wavelength.

In the specific case of normalisation, if it coincides between two ECG signals, it means that the signals have been adjusted to have the same amplitude and baseline, making them more comparable. It is visible in the graph of Figure 3 that there is a 100% coincidence between the signals, managing to perfectly analyse the variations in the same timings in both signals.

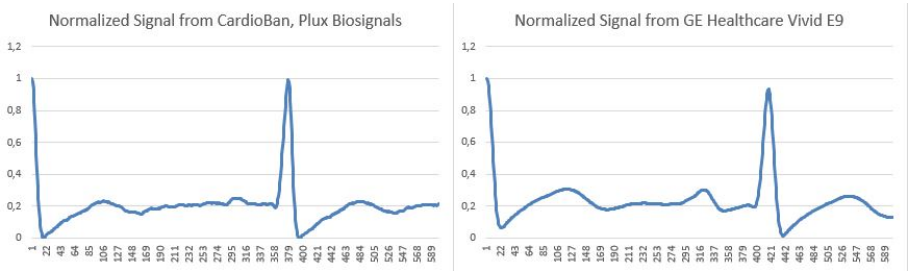


Fig. 3: ECG signal plot after normalising the data using the Excel tool. On the left, the normalized wavelength of the signal from CardioBan, Plux Biosignals and on the right, the normalized wavelength of the signal from GE Healthcare Vivid E9.

5 Conclusion

The review assessed the potential of the Cardioban device by Plux Biosignals for monitoring cardiovascular health in clinical practice and research. The study found that the Cardioban performed comparably well to a certified clinical device in detecting early warning signs of heart disease. Wearable medical devices like the Cardioban have the

potential to provide valuable real-time insights into a user's health status. The accuracy of wearable medical devices, especially those for medical purposes, is critical to avoid misdiagnosis and improper treatment. Wearable devices for remote patient monitoring are more important now during the COVID-19 pandemic. This study provides valuable insights into the Cardioban's accuracy and effectiveness for monitoring cardiovascular health, suggesting the potential of wearable medical devices for cardiovascular health monitoring. Further research is needed to investigate the Cardioban's potential in different populations and clinical settings.

6 Acknowledgements

This project was funded by the projects "NORTE-01-0145-FEDER-000045" and "NORTE-01-0145-FEDER-000059", supported by Northern Portugal Regional Operational Programme (Norte2020), under the Portugal 2020 Partnership Agreement, through the European Regional Development Fund (ERDF). It was also financed by national funds, through FCT - Foundation for Science and Technology and FCT / MCTES under the project UIDB / 05549/2020, UIDP/05549/2020, CEECINST/00039/2021 and LASI-LA/P/0104/2020. This project was also funded by the Innovation Pact HfFP – Health From Portugal, co-funded from the "Mobilizing Agendas for Business Innovation" of the "Next Generation EU" program of Component 5 of the Recovery and Resilience Plan (RRP), concerning "Capitalization and Business Innovation", under the Regulation of the Incentive System "Agendas for Business Innovation".

References

1. G. Prieto-Avalos, N. A. Cruz-Ramos, G. Alor-Hern´andez, J. L. S´anchez- Cervantes, L. Rodrıguez-Mazahua, and L. R. Guarneros Nolasco, "Wearable Devices for Physical Monitoring of Heart: A Review," Biosensors (Basel), vol. 12, no. 5, May 2022, doi: 10.3390/BIOS12050292;
2. "cardioBAN — biosignalsplux Datasheet CARDIOBAN20220922," 2022, Accessed: March, 2023. [Online]. Available: http://biosignalsplux.com/;
3. G. S. Lazaretti, J. P. Teixeira, E. V. Kuhn, and P. H. Borghi, "Android-based ECG monitoring system for atrial fibrillation detection using a BITalino ECG sensor," pp. 177–184, Feb. 2022, doi: 10.5220/0010905400003123;
4. E. Sitompul, A. Suhartomo, F. Darmawan, N. S. Syafei, and A. Turnip, "Prototype of Portable Heart Monitoring System using BITalino," ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, Teknik Elektronika, vol. 11, no. 1, p. 31, Jan. 2023, doi: 10.26760/elkomika. v11i1.31;
5. "Training Manual GE Logiq Vivid E9 PDF - Medical Ultrasound - Power Supply."https://pt.scribd.com/document/425081670/ Training - Manual - GE - Logiq - Vivid E9 - pdf (accessed March, 2023);
6. AKumar, N., Verma, N., & Singh, A. (2020). Wearable Devices for Early Detection of Cardiovascular Diseases: A Comprehensive Review. Journal of Medical Systems, 44(11), 1-12. doi: 10.1007/s10916-020-01661-8.

Smart Crosswalk Accessibility for the Visually Impaired

Facundo M. Bustos C.[1] and João Paulo Coelho[1,2,3]

[1] Polytechnic Institute of Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal.
[2] Research Center for Digitization and Intelligent Robotics (CeDRI). Polytechnic Institute of Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[3] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
jpcoelho@ipb.pt

Abstract. The exponential growth of urban populations has put in agenda the need of cities to become more sustainable. The concept of *Smart Cities* can be an important part for the solution to this problem. One of the elements that can be found in this paradigm are smart crosswalks. Although they have many advantages, it is still difficult to adequately support people who are blind or visually impaired when they are crossing the street. This paper addresses this problem by presenting a project that aims to develop a solution to promote accessibility of visually impaired citizens through the implementation of a digital fencing system based on the user location obtained from the RSSI values between two beacons and the user's smartphone. Details behind its architecture and the overall functionality of a custom-made app will be provided.

Keywords: Pedestrians crosswalks accessibility· Digital fencing · Smart Cities · Bluetooth Beacons

1 Introduction

Over the past 50 years, the population living in cities has grown quickly, and by 2050, it is predicted that almost two-thirds of the world's population will live in urban areas [1]. *Smart Cities* has emerged as a solution to address the pressing need for cities to become more sustainable, efficient, and livable. *Smart cities* are urban areas that uses Information and Communication Technologies (ICT) services or products that: enhance the social and ethical well-being of its citizens; provide quality, performance, and interactivity of urban services to reduce costs and resource consumption; and increase contact between citizens and government [2].

The installation of smart crosswalks is one of the key elements of *smart cities*. Using a variety of technologies, smart crosswalks are an intelligent traffic management system that aims to improve pedestrian safety, reduce traffic congestion, and enhance overall pedestrian experience.

Although Smart Crosswalks have many advantages, it is still difficult to adequately support people who are blind or visually impaired when they are crossing the street. According to the most recent national censuses, in Portugal about 890,000 people have vision problems, of which 27,000 are totally blind [3]. The lack, or significant deprivation of the sense of sight, translates into challenges that some people must overcome and that are normally not perceived by the rest of the population. The sharing of space between cars and people poses safety challenges that must be considered to avoid accidents that often end in fatalities. Security is even more critical on crosswalks since these are

places where the probability of collision between vehicles and pedestrians is substantially higher. Knowing when and where it is safe to cross a given road is fundamental.

This work seeks to include active systems that could promote an increase in crosswalks safety targeting a broader pedestrian universe of users which includes visually impaired persons. This accessibility module is intended to be integrated in the future into the VALLPASS project. This project developed a pedestrian crosswalk that it is integrated into the smart cities paradigm.

The aim of this paper is to describe the overall approach that will be taken to increase the smart pedestrian crosswalk accessibility to visually challenged pedestrians. Details regarding the technological tools used to achieve this solution will be provided in Section 3. Before that, an overview of related work is presented in Section 2. Then Section 4 explores the accessibility approach. In Section 5 it is showed the experimental test made. And last, the closing section will be devoted to presenting the main conclusions of the paper and pointing out further work directions.

2 Related Work

This section will be devoted to describing the most common approaches found in the literature that deal with the problem of crosswalks accessibility improvement for visually impaired pedestrians. The solutions are found to fall into one of the following two categories: global positioning using GNSS/GPS and image processing.

[4], designed a smartphone application that takes the user location and orientation obtained from the GPS receiver and for the cases where the GPS signal is weak, they placed Bluetooth beacons with a geo-ID tag to improve the information on the user's location. The application exchange messages with the traffic light controller asking how long the user must wait until is safe to cross the road. This information will then be relayed to the user using audio messages. It is worth pointing out that this approach requires the location of Bluetooth beacons since, in general, they are not integrated into the conventional crosswalk signaling system. Moreover, it relies on the availability of an API to query the traffic system about its status which is not usually the case.

Other researchers approached this question through computer vision and image processing. That is the case of the research made by [5], they worked on the Crosswatch project. They first identify the intersection where the user is standing in through the GPS sensor of the smartphone. Then it asks the user to rotate to take a panoramic image of the location. Then, they obtain a second image from Google Maps of the intersection. With these two images they run a computer vision algorithm to do a comparison between them and obtain the exact location of the user. The focus of this project is to obtain the exact location of the user, that information later could be used as a base for future work to help to guide to user go through the intersection, but the image capture method maybe it's too complicated to be performed by a visually impaired. Another problem with this kind of solution is that they rely on the user smartphone and its capabilities of performing a fast image processing to be able to locate the user in real-time.

Kiyoung et al. [6] presented the Crossing Assistance System (CAS) where a location is performed through machine learning using the Received Signal Strength Indication

(RSSI) from eight Bluetooth beacons located at a four-corner car intersection with four crosswalks (two beacons at each side of a crosswalk). A smartphone app takes the measured RSSI of each beacon and then the machine learning algorithm computes the user location. In this setup, the beacons send data every half second and the smartphone app is built to receive two RSSI signals per second provided by the eight beacons. As they have large amounts of data, and the signals can be sensitive to noise due to the traffic they implemented the moving average filter to achieve better results. According to the authors, if they give the algorithm a three seconds windows to process the data, they can provide the user location with a $99,8\%$ accuracy. However, their work doesn't implement any guidance system as their main focus was developing the location algorithm, although they mention it as a potential future work. In addition, Bluetooth beacons must be installed on third party systems which can be challenging.

3 System Architecture

In this section we explore the technological tools used for the approach taken in this project.

3.1 BLE Beacons

Bluetooth beacons are transmitter devices that broadcast a BLE signal to the nearby mobile devices. This technology enables other devices to perform actions when near to one of them.

One of the main differences between Bluetooth beacons and other location-based technologies is that the beacons are an unidirectional transmitter: it can't receive data. Thus, it is needed that the receiving devices have a specific application or system to interact with the beacon. This warranties that only the application is able to track the user location and not the beacon transmitter [7].

To transmit data to the receivers, the beacons use the advertising mode to broadcast data periodically. The advertising signals contains a small data payload, also known as Protocol Data Unit (PDU) [8]. The selected protocol for this project is shown in the Figure 1.

(a)	Adv PDU			Payload defined by iBeacon Standard				
1 byte	4 bytes	2 bytes	6 bytes	9 bytes	16 bytes	2 bytes	2 bytes	1 byte
Preamble	Access Address	Header	MAC	iBeacon Prefix	Universally Unique Identifier (UUID)	Major	Minor	Tx Power

Fig. 1: Advertising PDU of iBeacon. Image from [9].

3.2 Distance measurement

The average signal power between a transmitter and a receiver decreases logarithmically with distance. The RSSI indicates the energy loss in the signal transmission. The smaller

the value, the less the attenuation. One of the most commons methods of RSSI ranging, and the one used in this work, is the shadowing model.

The logarithmic normal distribution describes the random shadowing effects which occur due to the environment on the propagation path [10].

$$P_L(d) = P_L(d_0) + 10n \log(\frac{d}{d_0}) + \chi_\sigma \tag{1}$$

Operating in the Equation 1 and knowing that d is the undetermined distance [11]:

$$d = 10^{(A-RSSI)/10n} \tag{2}$$

3.3 RSSI filtering

To be able to obtain the distance to a beacon using the Equation 2 we need to eliminate the uncertainty generated by the random variable χ_σ. To solve this problem, in this work we use the moving average filter. It is a statistic filter that works by gathering n RSSI samples and averaging the values to create a new value.

$$\overline{RSSI} = \frac{1}{n} \sum_{i=0}^{n} RSSI_i \tag{3}$$

4 The accessibility approach

The VALLPASS project have developed and built a smart pedestrian crosswalk solution that improves the security of pedestrians and, at the same time, is compatible with the *smart cities* ecosystem. The situation illustrated on the Figure 2 presents the typical disposition of the VALLPASS solution.

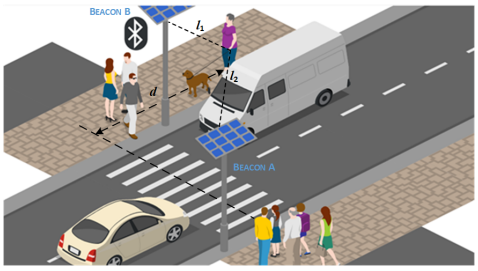


Fig. 2: The VALLPASS smart pedestrian crosswalk.

In the VALLPASS smart crosswalk solution, there are two VALLPASS units installed sideways of a crosswalk. Each one of the VALLPASS elements includes BLE beacon, configured with the *iBeacon* protocol that broadcast a RF signal able to be detected by every device that is near to it. Assuming that a given pedestrian has a smartphone with the designed application installed, the advertised PDU and the RSSI of each beacon

will be decoded by the software and the relative position of the pedestrian, regarding the crosswalk, is estimated.

It is worth noticing that, in practice, location by triangulation requires, at least, three points. However, in a typical crosswalk application, only two VALLPASS units will be available. Hence, there is an intrinsic uncertainty if the pedestrian is upstream or downstream of the crosswalk. However, this issue is not fundamentally a problem since the location algorithm will be concerned with the relative peak power and disregard if the pedestrian is approaching the center of the crosswalk from the left or from the right. Moreover, positioning is not the main objective of this system. Indeed, pedestrian positioning can be fine-tuned by himself with the help of the tactile cues embedded on the sidewalk. Being able to provide accurate information on the actual crosswalk and traffic status while providing decision support regarding the most secure time interval to cross the road is the key feature of the accessibility system.

4.1 Android Application

Figure 3 shows the basic flowchart of how this application works. To be able to interact with the visually impaired it implements text-to-speech of the distance every 10 seconds.

The UI of this application, it contains the main information of the nearby Beacons. It can be seen in Figure 4.

There is an implementation of a text-to-speech of the distance to the crosswalk allows the interfacing with the visually impaired.

5 Results

From (2) it is needed to determine the RSSI at one meter, and the path loss exponent (n). From experimental testing these values are:

- $A = -62dBm$
- $n = 3$

5.1 Experimental Testing

Once the application is configured with all its parameters, some tests on the system were performed in an urban landscape with little signal interference's (such as cars and pedestrians). For this purpose, the device was submitted to take one hundred measurements, and four tests were performed. For each test, the window size of the moving average filter was the following:

- Test A= 1
- Test B= 3
- Test C= 5
- Test D= 10

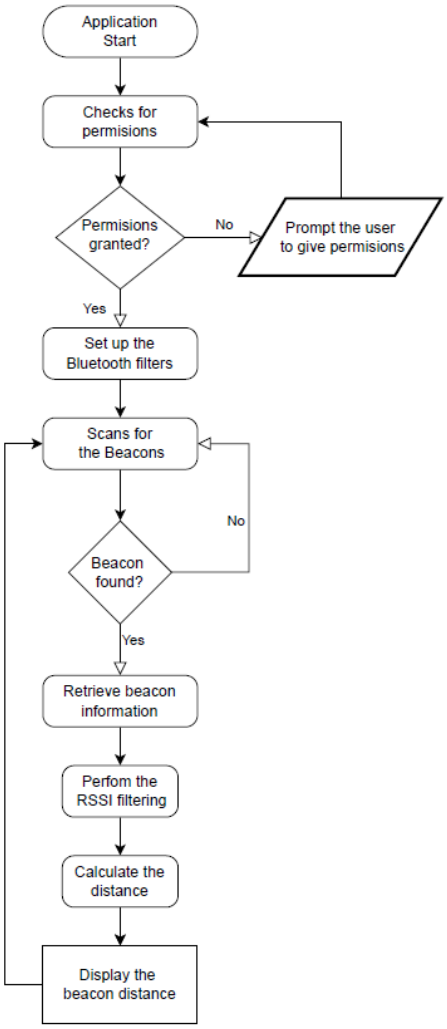


Fig. 3: Structure of the Android APP

5.2 Analysis of the Experimental Results

In Figure 5 it is presented the measurement results with the beacon placed at 10 meters from the phone.

One factor that is needed to understand the behavior of the system is the coefficient of variation (CV) which is a statistical measure that represents the relative variability or dispersion of a dataset, expressed as a percentage. It is calculated as the ratio of the standard deviation to the mean of the dataset. The Figure 6 show the coefficient of variation for the measurement with the beacon placed at 10 meters from the phone.

The Figure 7 present the systematic error from the test performed at 10 meters of distance.

From the analysis, tests C and D have demonstrated promising results, principally for test D, in which it has shown the lowest systematic error and standard deviation. However, these results can mislead the true performance of the system. It cannot be left

Fig. 4: UI of the Android APP

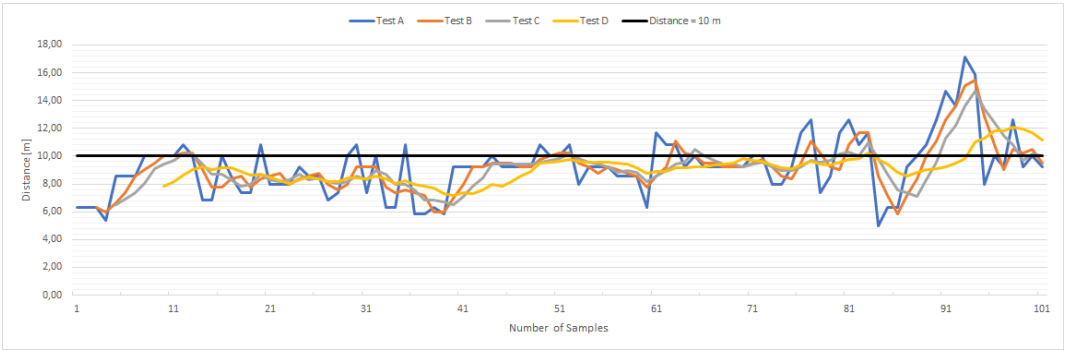


Fig. 5: Analysis with the beacon at 10 m from the phone.

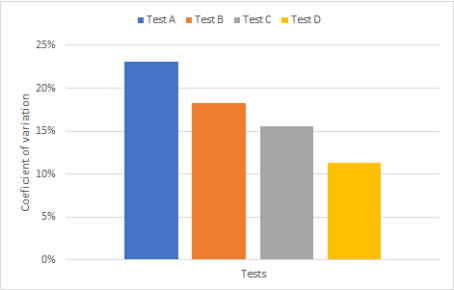


Fig. 6: Coefficient of variation from the beacon at 10 m from the phone.

unnoticed that these tests were performed in a condition where the distance between the beacon and the phone was constant, as they were in a fixed position. With a bigger window size in the moving average filter the less the resulting data will be influenced by the variation due to noise, meaning a better precision. But this comes at the cost of a slower reaction time for the system to display and communicate with the user its actual location, as this filter does not have the ability to distinguish between noise and real data variations.

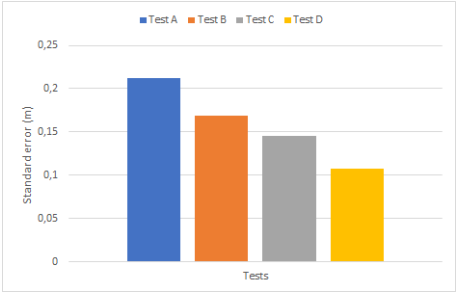


Fig. 7: Average systematic error presented from the beacon at 10 m from the phone.

6 Conclusion and Future Work

Modern societies are inclusive by definition and promoting life quality of all persons should not be a question of numbers. At the present, where societal digitalization is accelerating, efforts must be made to use that technology to further improve the urban mobility and accessibility of persons with disabilities. It is framed on this idea that this project seeks to develop a smart pedestrian crosswalk that has security as a major concern. One of the key concepts of this solution is the inclusion of active security measures targeting visually impaired persons.

This approach have been done using BLE beacons as a reference point for the location of the crosswalk, and an application that exchanges information with the beacons and communicates with the user.

The performance of the system is not the ideal as even in a controlled environment there were signal noise that caused errors at the moment to calculate the distance between the beacon and the phone. But it is worth pointing out that even if the distance calculation where not precise, they should provide an estimation of the user location (relative to the crosswalk) and with more development able to determine when the pedestrian is near a crosswalk and then communicate relevant information to them such as traffic status and if it is safe to cross; this data can be gathered by the systems already installed into the VALLPASS units.

Further steps on this work, is the integration of the explored solution to locate the user with the existing VALLPASS units to be able to query the system to get information on when to cross the road and communicate with the user. Also is worth exploring other communication method besides text-to-speech, such as haptic approaches using the smartphone touchscreen and vibration actuator.

Acknowledgment

The authors are grateful to the project VALLPASS (vigilância ativa e inteligente com suporte LoRa para passadeiras), NORTE-01-0247-FEDER-113439, for supporting this work.

References

1. Hannah Ritchie and Max Roser. Urbanization. *Our World in Data*, 2018.

2. Rebecca Hammons and Joel Myers. Smart cities. *IEEE Internet of Things Magazine*, 2(2):8–9, 2019.
3. Instituto Nacional de Estatística (Statistics Portugal). Resident population with at least one difficulty aged 5 years or over according to the type and degree of difficulty experienced, by number of difficulties per person, age group and sex., 2011.
4. Chen-Fu Liao. Mobile accessible pedestrian signals (maps) for people who are blind. *18th ITS World Congress, Orlando, Florida*, 2011.
5. Vidya Murali and James Coughlan. Smartphone-based crosswalk detection and localization for visually impaired pedestrians. *IEEE Int Conf Multimed Expo Workshops*, 2013.
6. Kiyoung Shin, Ryan McConville, and Oussama Metatla. Outdoor localization using ble rssi and accessible pedestrian signals for the visually impaired at intersections. *Sensor*, 2022.
7. Ellisys. Bluetooth beacons.
8. Intro to bluetooth generic access profile (gap).
9. Kang Eun Jeon, James She, Perm Soonsawad, and Pai Chet Ng. Ble beacons for internet of things applications: Survey, challenges, and opportunities. *IEEE Internet of Things Journal*, 5(2):811–828, 2018.
10. Theodore S Rappaport. Wireless communications–principles and practice, (the book end). *Microwave Journal*, 45(12):128–129, 2002.
11. Fengjun Shang, Wen Su, Qian Wang, Hongxia Gao, and Qiang Fu. A location estimation algorithm based on rssi vector similarity degree. *International Journal of Distributed Sensor Networks*, 10(8):371350, 2014.

Carpentry Digital Transformation: Woodwork 4.0 in Industry 4.0

Iaggo Capitanio[1], Nuno Guedes[3], João Paulo Coelho[1,3], Nélio Pires[4], João Magalhães[5], and Higor Vendramini Rosse[5]

[1] Research Center for Digitization and Intelligent Robotics (CeDRI). Polytechnic Institute of Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
iaggo.capitanio@gmail.com, jpcoelho@ipb.pt
[2] Laboratory Collaborative Mountains of Research, Bragança, Portugal.
nguedes@morecolab.pt, hrosse@morecolab.pt
[3] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[4] Carpintaria Mofreita Lda., Maceido de Cavaleiros, Portugal
fm.mofreita@mofreita.com
[5] New Knowledge Advice Lda., Braga, Portugal
joao.magalhaes@nka.pt

Abstract. The digital transformation of an enterprise, especially those deeply rooted in traditional practices such as carpentry, is a multifaceted challenge extending beyond mere technicalities to encapsulate corporate identity and its broader business ecosystem. The fourth industrial revolution, contrary to its predecessor which yielded tangible productivity gains through mechanization, is driven by data and interconnections, making the immediate benefits elusive and difficult to comprehend. Key to this transition is the promotion of digital twinning, fostering a seamless integration between physical assets, humans and data. Recognizing the unique needs of each business, digital transformation necessitates bespoke solutions rather than a one-size-fits-all approach. Against this backdrop, this paper introduces the Woodwork 4.0 project, an open-source initiative funded by the Portuguese NORTE2020 program, which is geared towards the digitization of a small to medium-sized carpentry business. The paper delves into the specific challenges encountered, elucidates the architecture of the proposed system, and offers insights into the practicalities of deploying digital solutions in the context of traditional industries.

Keywords: · Digital Transformation · Woodwork 4.0 Project · System Architecture for Digitization · Fourth Industrial Revolution · Carpentry Industry Digitalization.

1 Introduction

The conventional depiction of a small-scale carpentry workshop, characterized by skilled artisans laboring to meticulously craft wooden items, has experienced a transformative shift in the 21st century. This metamorphosis is particularly evident in the Mofreita carpentry shop in North East Portugal. In the present day, the adoption of computer numerical control (CNC) milling machines has revolutionized the traditional woodworking operations, enabling extraordinary levels of precision and customization in line with customers' unique requirements [1]. This customer-centric methodology, amalgamated with lean production techniques, has incited significant alterations in custom-made manufacturing.

Despite these advancements, the sector demands further digitalization of its processes, aiming to minimize waste and enhance process control. Consequently, this study

proposes to address these objectives through the comprehensive digitization and traceability of carpentry processes.

Nevertheless, there exists a conspicuous lack of scholarly exploration focused on the digitalization of wood manufacturing. A work that bears similarity to the present study is conducted by [2], wherein the authors developed a platform capable of consolidating information related to the wood extraction process [3, 4]. However, this study, akin to others, restricts its scope merely to the supply chain process. Consequently, the intent of this project is to bridge this gap in academic research and contribute to the growth and development within this under-explored field.

The fusion of physical production with the digital sphere—marked by the harnessing of real-time data, machine learning algorithms, and big data analytics—is a distinctive feature of the Fourth Industrial Revolution [5–8]. However, the adoption of this approach necessitates a fundamental prerequisite step—the digitalization of all processes. Commercial entities, such as the Mofreita carpentry shop, grapple with the challenge of integrating such a comprehensive scope of information into their distinctive manufacturing processes. An efficient information processing infrastructure that can effectively manage data sourced from CAD/CAM software, inventory availability, and shop-floor traceability is crucial. Equally important is the establishment of systems capable of integrating residual woodcuts back into the production cycle, thereby contributing towards waste minimization and recycling efforts.

In this context, the Woodwork 4.0 (WW4.0) project, financed by NORTE 2020, was initiated to expedite Mofreita's digitization and serve as a blueprint for similar enterprises. The project emphasizes traceability, both in raw material management and production process tracking, and includes real-time information on leftover woodcuts and the capability for customers to remotely track their orders.

This paper presents the WW4.0 project's ontology and comprehensive architecture. It begins by exploring contemporary smart factory concepts (Section 2), followed by an analysis of Mofreita's existing manufacturing processes (Section 3). The transformative potential of the WW4.0 project is discussed in Section 4, leading to an overview of the proposed system architecture and ontology. The paper concludes with key findings, conclusions, and suggestions for future work (Section 5).

2 Modern Solutions to Traditional Challenges: The Smart Factory

Practices for continuous improvement such as lean management have become integral for companies aiming to optimize operations amidst strong competition and economic instability [9]. Despite the advancements in information technology, there remain challenges, notably in real-time monitoring and control of internal and external material flows [10]. To tackle this, automatic identification systems (AIS) employing technologies like bar-codes and radio frequency identification have been widely adopted [11] [12] [13].

However, implementing the smart factory concept is complex due to the diverse operational conditions of companies. There are no universal digitization solutions, and technologies often require significant adaptation and customization before integration into existing production processes. Small and medium enterprises (SMEs) face these

digitization challenges more acutely due to their limited resources and technical expertise.

In this context, the Woodwork 4.0 project was developed with the primary aim of creating a tailored digitization methodology for the *Monfreita* company. It is envisioned that the methodology and steps used for this transformation can serve as a guide for similar manufacturing industries in their digitization journeys.

The next section will delve into the current workflow of the *Monfreita* company, providing insight into the challenges inherent in each process step.

3 The Carpentry 4.0 Workflow and Challenges

The *Mofreita* carpentry, like many similar companies, requires a diverse workforce to carry out various tasks ranging from management to production-centric roles such as CAD design and furniture assembly. These roles demand and generate distinct sets of information, necessitating a two-way flow of information. Current communication methods and inventory management practices are traditional, leading to several challenges, such as the reintegration of leftover wood boards from previous processing stages into new projects and lack of precise historical data for forecasting man-hours for new projects.

The company faces difficulties in recording and tracking the characteristics and location of leftover wood pieces. Also, reliance on individual operator knowledge leads to inconsistencies in stock availability information.

To address these challenges, the implementation of a comprehensive digital system consolidating all project components is proposed. The aims of such a system would include enhancing information flow, creating a centralized repository for each client's projects, recording time required for each processing stage, maintaining a registry of characteristics and physical location for all wood board remnants, improving traceability and management of various consumables, and providing clients the ability to remotely monitor the project's progress via a web-based user interface.

Accurately retrieving the time required for each step in a client's project is challenging in practice. While expertise can provide rough estimates, precise historical data would improve the prediction of man-hours needed for new projects during the budgeting phase.

The solution seems to be a digital system that unifies all project components, intending to:

- Enhance information flow within different offices and the shop floor;
- Establish a repository for each client's projects, containing CAD, CAM, budgets, and additional documentation;
- Track the time required for each processing stage per project;
- Maintain a registry of the characteristics and physical location of all leftover wood boards for potential future use;
- Improve traceability and daily management of consumables such as fixtures, sandpaper, glue;

– Enable clients to remotely follow the project's progress via a web-based user interface.

These issues can be addressed using typical approaches found in Industry 4.0 paradigms, specifically process digitization, management and logistics integration, and traceability improvement. The subsequent section will present the architecture for a Carpentry 4.0 model extended from some Industry 4.0 concepts.

4 Overall Architecture for the Carpentry 4.0

The Industry 4.0 concept revolves around interconnecting diverse processes through fully connected devices. Applying this concept to carpentry entails establishing access to files generated by various third-party software and enabling integrated stock management with a high degree of digitalization [14].

The proposed work aims to create an information aggregation and processing platform for sharing information among actors in the production process. This includes exchanging information about available raw materials and wood parts to be processed. By utilizing optimization algorithms, optimal raw material management can be achieved, leading to waste reduction, increased production, and cost savings.

Figure 1 presents an architectural overview of the WW4.0 platform, the central information system housing data associated with current and past projects.

The WW4.0 platform serves as a hub for aggregating relevant production process data and facilitating information sharing among various software applications. It optimizes raw material management by cross-referencing stock data with wood parts lists. Allocation optimization is achieved through the application of optimization algorithms.

Practically, the production cycle involves different software applications, such as 3D modeling and CAD/CAM, which generate cutting lists and machine code for nesting and CNC machines. The WW4.0 platform stores these files and makes them accessible to operators on the factory floor. Additionally, based on stock information, including leftover and raw materials, the WW4.0 platform can suggest suitable materials for production cutting lists, thereby automating the raw material assignment process.

As mentioned in Section 3, *Mofreita*, like many similar businesses, does not utilize ERP software due to its lack of necessary functionalities and adaptability to carpentry SMEs. Stock management is currently done using spreadsheets. To address this, a patch will be developed to enable remote control of spreadsheet data, allowing the WW4.0 platform to interact with stock information via Restful API. Figure 2 illustrates this approach.

Monitoring applications facilitated by supervision software services are integral to the operational efficacy of the Woodworking 4.0 (WW4.0) core context management system. These applications are chiefly responsible for the detection of alterations within data files housed in distinct folders. Upon identifying such changes, they promptly initiate updates in the WW4.0 management system.

In the existing framework, the management of context information associated with all client projects will be handled by FIWARE® [15]. This is an open-source platform

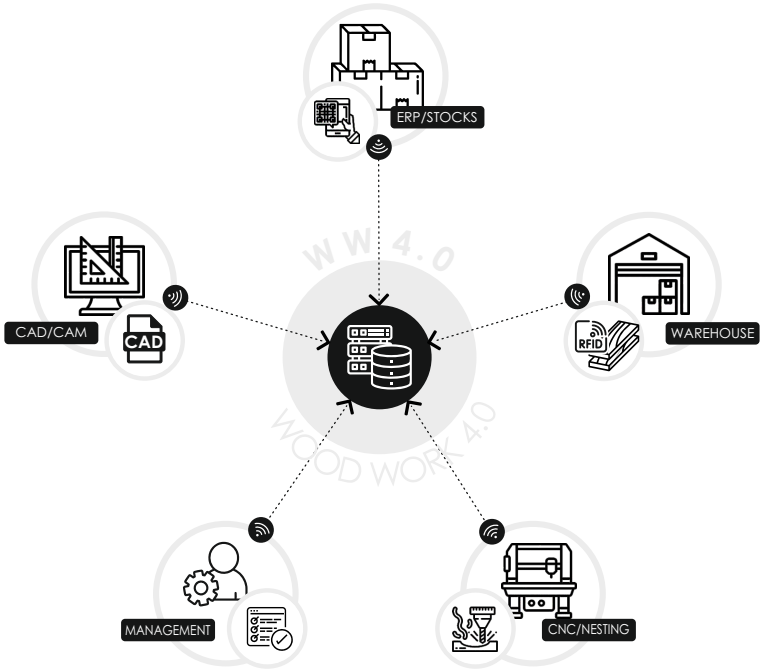


Fig. 1: Architectural overview associated with Carpentry 4.0.

widely used for developing intelligent solutions, digital twins, and various other digital transformation applications [16–18].

The core service of WW4.0 relies on the Orion context broker, responsible for managing the contextual information received from APIs and devices. This service is complemented by the Watchdog application and Bucket API, which extract data from folders and serve static files, respectively.

In the current architecture, depicted in Figure 3, each project is represented as a digital entity within the context broker. Attributes such as completion stage and processing times are maintained and managed by the context broker.

Ensuring the security of contextual information is another crucial aspect. To address this, the WW4.0 apiary is built using Django technology, providing authentication for external users as clients of the Keyrock IDM (Identity Manager). This combination of technologies ensures layered authentication and authorization, allowing controlled access to specific pages or resources based on user roles. Keyrock serves as a centralized authentication and authorization service, managing access to resources like Orion API endpoints, albeit without fine-grained control over user access.

The functionalities offered by FIWARE® enable the concept of intelligent products [19], wherein all production chain information is aggregated with the real-time status of the factory floor. This digital representation aligns with the concept of a digital twin, providing insights into the current production stage, estimated completion time,

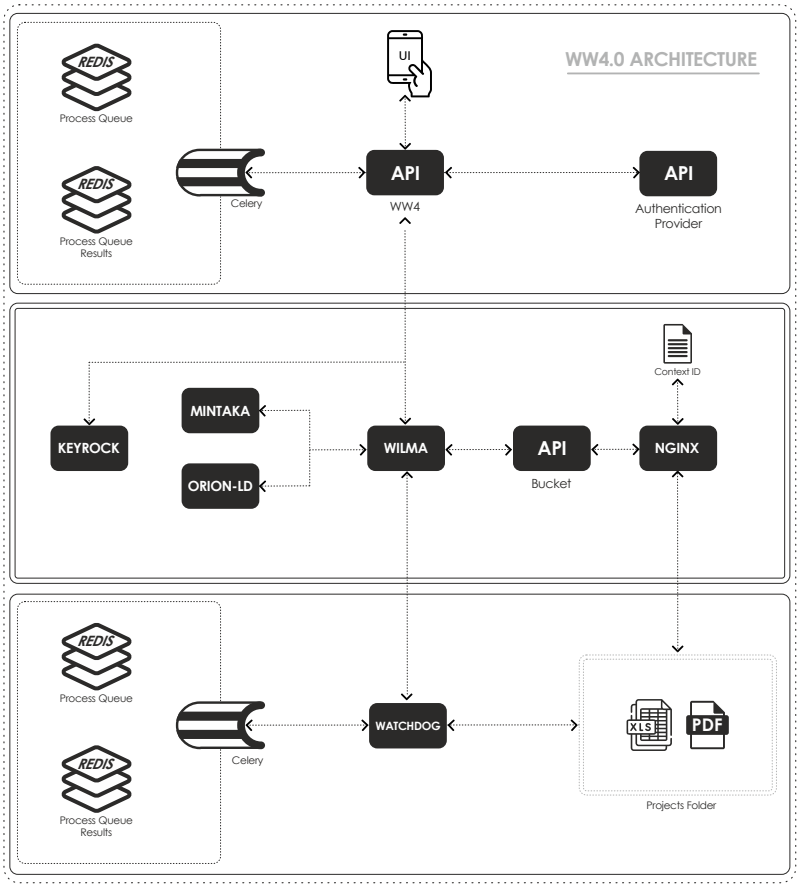


Fig. 2: Information democratization using software bridges between third-party software packages.

materials used, and more [20]. This information can be accessed remotely through web-based applications. Figure 3 visually illustrates this concept.

Ensuring traceability is a significant challenge posed by Industry 4.0. The seamless circulation of real-time information across workstations and auxiliary devices operated by personnel is crucial. In this regard, FIWARE® facilitates these tasks by consolidating the information flow through a centralized context broker agent. This enables the generated information from various departments to be universally accessible at different hierarchical levels, not only at the management level but also on the shop floor. The WW4.0 platform plays a crucial role in enhancing the traceability of parts and fixtures.

The fusion of various services to form an integrated ecosystem yields a multifaceted solution, capable of automation and real-time data processing. This system enhances the operational functionality within a manufacturing environment, enabling the automatic provision of project progress updates, seamless file sharing across different sections of the factory floor, and a dedicated communication system with customers. The Web interface developed in this project can be seen in Figure 4

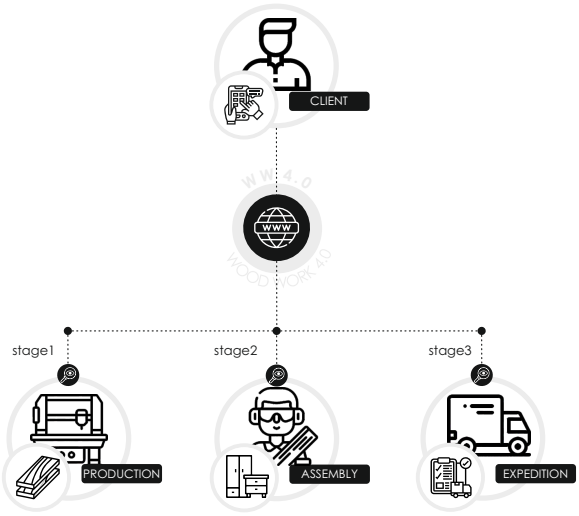


Fig. 3: Diagram that shows the WW4.0 platform functionalities within the intelligent product scope.

Furthermore, the solution encompasses mechanisms to provide instant notifications of design changes, ensuring up-to-date information flow and timely adjustments in the production process. Beyond these capabilities, the integrated ecosystem is designed to be future-proof. It allows for subsequent integration of an array of Internet of Things (IoT) devices, thereby providing a scalable solution. This capacity for expansion not only enhances current operational efficiencies but also ensures the system's adaptability to future technological advancements, maintaining its relevance in an ever-evolving digital landscape.

5 Conclusions and Further Work

The digital transformation of SMEs presents unique challenges due to their diverse organizational structures. While a universal plug-and-play solution may not be feasible, industries with similar typologies, such as carpentry, can benefit from integrated information infrastructures. The Woodwork 4.0 project aims to address this need by developing an information platform for carpentry industries.

This article presented the architecture of the WW4.0 information platform, which supports data generated throughout the production process. Key to this architecture is the utilization of FIWARE® as the context management element, along with various glueware applications that facilitate context sharing between FIWARE® and third-party software packages. To validate this approach, the WW4.0 model will be deployed in the Mofreita carpentry, located in northeastern Portugal, for testing and validation.

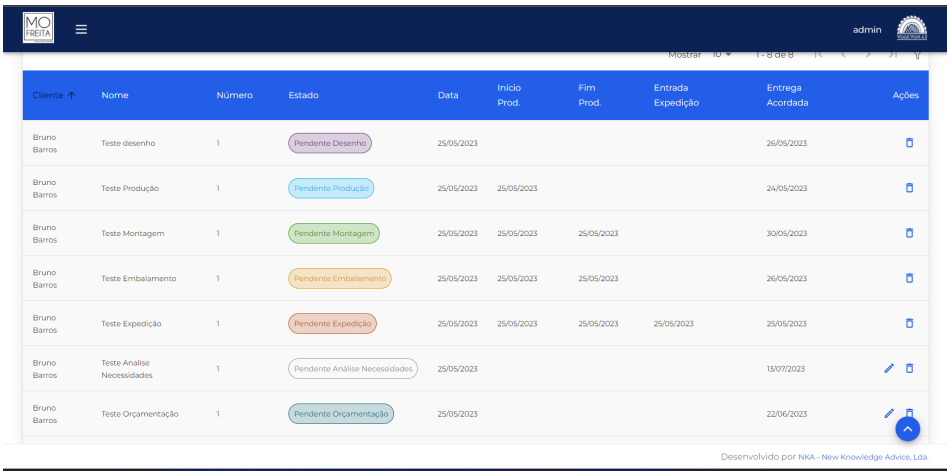


Fig. 4: User Interface platform to monitoring processes.

The next steps involve the technology transfer to the case study and the integration of a web-based front-end, currently in the testing phase, to serve as the graphical interface between the context broker and different user groups.

Acknowledgments

The authors acknowledge the support of NORTE - FEDER funds and Horizon 2020 for the Woodwork 4.0 project (NORTE-01-0247-FEDER-072593). Financial support from the Foundation for Science and Technology (FCT, Portugal) through national funds (FCT/MCTES) is also gratefully acknowledged for CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021).

References

1. Stephen J Rober and Yung C Shin. Modeling and control of cnc machines using a pc-based open architecture controller. *Mechatronics*, 5(4):401–420, 1995.
2. Edgar Diaz Amaya, Omar Troncos Rojas, and Mario Paiva Guerrero. Web solution based on qr code for the traceability of the wood transformation process. In *2022 IEEE XXIX International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4, 2022.
3. Janne Häkli, Kaarle Jaakkola, Pekka Pursula, Miika Huusko, and Kaj Nummila. Uhf rfid based tracking of logs in the forest industry. In *2010 IEEE International Conference on RFID (IEEE RFID 2010)*, pages 245–251, April 2010.
4. Yongke Sun, Guanben Du, Yong Cao, Qizhao Lin, Lihui Zhong, and Jian Qiu. Wood product tracking using an improved akaze method in wood traceability system. *IEEE Access*, 9:88552–88563, 2021.
5. Sandra Grabowska. Smart factories in the age of industry 4.0. *Management Systems in Production Engineering*, 28(2):90–96, 2020.
6. Khushbu Garg, Chandramani Goswami, R.S. Chhatrawat, Shyam Kumar Dhakar, and Govind Kumar. Internet of things in manufacturing: A review. *Materials Today: Proceedings*, 51:286–288, 2022. CMAE'21.
7. Wendy Arianne Günther, Mohammad H. Rezazade Mehrizi, Marleen Huysman, and Frans Feldberg. Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems*, 26(3):191–209, 2017.
8. Seung-Beom Son, Jun-Yeong Kwon, and Chae-Soo Kim. A study on solution oriented smart factory diagnostic system for sme. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 6101–6103, 12 2019.

9. Euclides Coimbra. Achieving excellence with kaizen and lean supply chains. *Total Flow Management*, 2009.
10. Paul Myerson. *Lean supply chain and logistics management*. McGraw-Hill Education, 2012.
11. Duncan McFarlane and Yossi Sheffi. *The impact of automatic identification on supply chain operations*. University of Cambridge, Department of Engineering, 2003.
12. Marco Altini, Davide Brunelli, Elisabetta Farella, and Luca Benini. Bluetooth indoor localization with multiple neural networks. In *IEEE 5th International Symposium on Wireless Pervasive Computing 2010*, pages 295–300. IEEE, 2010.
13. Sheng Zhou and John K Pollard. Position measurement using bluetooth. *IEEE Transactions on Consumer Electronics*, 52(2):555–558, 2006.
14. Fadi Shrouf, Joaquin Ordieres, and Giovanni Miragliotta. Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm. In *2014 IEEE international conference on industrial engineering and engineering management*, pages 697–701. IEEE, 2014.
15. FIWARE. FIWARE: The open source platform for our smart digital future, 2021. Accessed on: May 17, 2023.
16. Flavio Cirillo, Gürkan Solmaz, Everton Luís Berz, Martin Bauer, Bin Cheng, and Ernoe Kovacs. A standard-based open source iot platform: Fiware. *IEEE Internet of Things Magazine*, 2(3):12–18, 2019.
17. Álvaro Alonso, Alejandro Pozo, José Manuel Cantera, Francisco De la Vega, and Juan José Hierro. Industrial data space architecture implementation using fiware. *Sensors*, 18(7):2226, 2018.
18. Maria Angeles Rodriguez, Llanos Cuenca, and Angel Ortiz. Fiware open source standard platform in smart farming-a review. In *Working Conference on Virtual Enterprises*, pages 581–589. Springer, 2018.
19. Gerben G Meyer, Kary Främling, and Jan Holmström. Intelligent products: A survey. *Computers in industry*, 60(3):137–148, 2009.
20. Chien Yaw Wong, Duncan McFarlane, A Ahmad Zaharudin, and Vivek Agarwal. The intelligent product driven supply chain. In *IEEE international conference on systems, man and cybernetics*, volume 4, pages 6–pp. IEEE, 2002.

LMW-Database for compounds present in mushrooms

Carlos SH Shiraishi[1,3], Luan Castro[4], Miguel A. Prieto[3], Lilian Barros[1,2], Isabel C.F.R. Ferreira[1], and Rui MV Abreu[1,2]

[1] Centro de Investigação de Montanha (CIMO), Instituto Politécnico de Bragança, Portugal
shiraishi@ipb.pt
[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
[3] Nutrition and Bromatology Group, Universidad de Vigo, Spain
[4] Faculdade de Tecnologia e Análise de Desenvolvimento de Sistemas, Integrado, Campo Mourão, Paraná, Brasil.

Abstract. This study focuses on the potential of mushrooms as a source of medicinal compounds. It describes the construction of LMW-Database compounds present in mushrooms (`https://cshiraishi.github.io/LMW-Database/`). Mushrooms, traditionally valued for their medicinal properties, have received scientific confirmation of their potency, resulting in the identification of a diversity of compounds with therapeutic applications. However, efficient access to these compounds for modern drug research has been challenging. The LMW-Database Database emerges as an answer to this challenge, serving as a dedicated platform for making mushroom compounds available for virtual drug and inhibitor discovery screening. As prospects, we plan to expand the LMW-Database Database to incorporate compounds from other natural sources, such as marine fungi and plants such as fig, potentially accelerating new drug discovery by increasing the diversity of compounds available for study.

Keywords: Mushrooms · Database · WEB.

1 Mushrooms and their medicinal properties

Medicinal mushrooms are said to possess approximately 130 therapeutic properties, including antitumor, immunomodulatory, antioxidant, cardiovascular, antihypercholesterolemic, antiviral, antibacterial, antiparasitic, antifungal, detoxifying, hepatoprotective, anti-diabetic, anti-obesity and anti-ageing activities, among others. High molecular weight compounds (HMW), as well as low molecular weight (LMW) compounds, present in these mushrooms, represent a vast and, for the most part, an underexplored treasure of powerful potential new drugs.s [1] [2], as represented in Figure 1.

Mushrooms are sources of low molecular weight (LMW) organic compounds such as quinones, cerebrosides, isoflavones, catechols, amines, and triacylglycerols. These compounds exhibit antitumoral and immunostimulant activities, stemming from the mushrooms' secondary metabolism and originating from intermediaries of the primary metabolism. These compounds can be categorized according to the biosynthesis pathway by which they are produced: (1) derived from amino acids, (2) the shikimate pathway for the biosynthesis of aromatic amino acids, (3) the acetate-malonate pathway of acetyl coenzyme A, (4) the mevalonic acid pathway of acetyl coenzyme A, and (5) polysaccharides and peptidopolysaccharides. It is important to emphasize that pathways (3) and (4) play a crucial role in producing these LMW compounds. This point

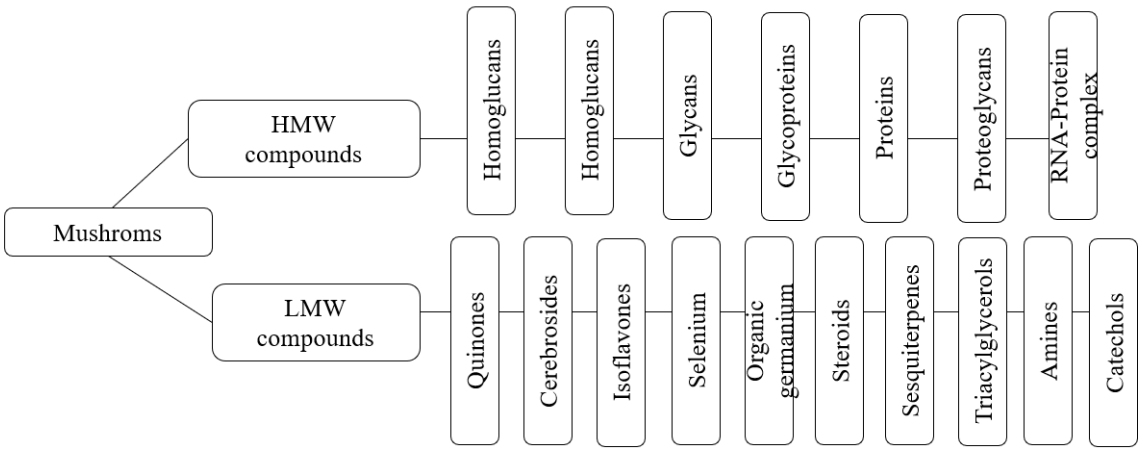


Fig. 1: Low molecular weight (LMW) and high molecular weight (HMW) compounds with antitumor potential found in mushrooms).

highlights the complexity of the chemistry of natural products and the intricate interaction between the various metabolic pathways involved in the biosynthesis of these valuable compounds. [2].

Mushrooms produce a variety of secondary metabolites, among which phenolic compounds stand out. These compounds, which contain at least one aromatic ring and one or more hydroxyl groups, are used by fungi and plants for protection against various factors, such as UV light and insects. About 8000 natural phenolic compounds are classified according to their structure and number of carbon atoms. [3].

In addition to their antitumor and immunostimulating properties, many of these compounds exhibit other medicinal activities. For example, certain quinones and isoflavones possess antioxidant and anti-inflammatory activities, cerebrosides may function as neuroprotective agents, and some catechols have potential antidiabetic capabilities. [2] [1].

The diversity and complexity of these compounds in mushrooms emphasize the need for a comprehensive and accessible database to catalogue and provide detailed information for each compound. Such a resource would be invaluable for researchers exploring the medicinal potential of mushrooms, accelerating the discovery of potential new drugs.

2 Databases of biological molecules

2.1 Databases of biological molecules: LMW Database

Several databases are used for virtual screening, which contains structures of a wide range of small molecules. They search for compounds that may interact with a biological target of interest. Examples include PubChem [4], ChEMBL [5], ZINC [6], and natural product databases such as Coconut Database [7]. Databases of naturally derived compounds have been continuously explored and valued by the scientific community due to their importance in natural products research.

The LMW Database (`https://cshiraishi.github.io/LMW-Database/`), similar to the databases above, is free and open access for all users, with no login required for entry. Its web interface facilitates various simple searches, such as search by molecule name. It also allows advanced search by molecular characteristics and also the download of the respective chemical structure.

3 Database Construction

3.1 Selection and preparation of compounds

Compounds with therapeutic activities derived from mushrooms were identified in scientific articles from the Scopus and Pubmed databases, subsequently drawn with the ChemSketch software (`www.acdlabs.com/resources/free-chemistry-software-apps/chemsketch-freeware/`) to obtain their SMILES format, which was later prepared using the OpenBabel program [8] and converted to .sdf format using the Datawarrior program [9], as represented in Figure 2.

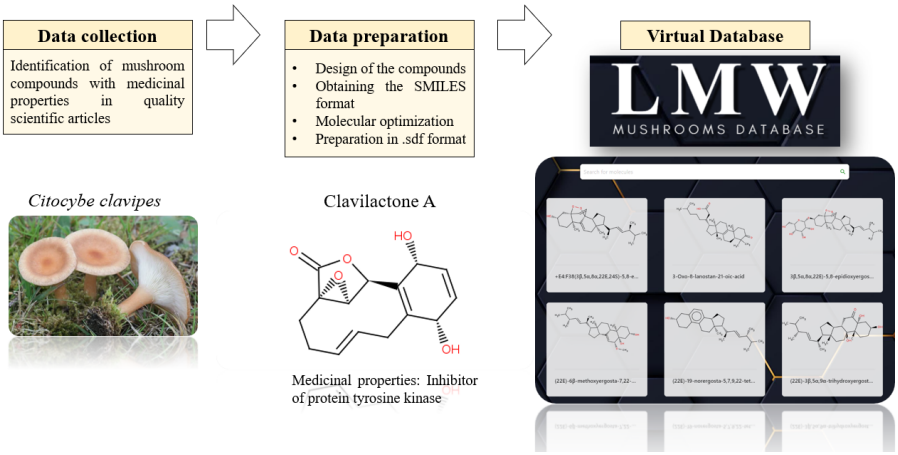


Fig. 2: Process of identification and preparation of compounds present in the LMW Database

3.2 Website Construction

In this process (Figure 3), a spreadsheet with molecular data is initially converted into a JSON file through a Python script. Subsequently, a ReactJS project is created, suitable for building web applications. Next, a list of molecules and a search bar are developed using the AntDesign tool. The molecular data are then visualized using Cards, and a button for downloading the molecule in .sdf format is provided, along with the display of the molecule image. Then, an iframe with the NGLViewer molecule viewer is displayed to load the .sdf file. Finally, the project is made available on the web using the GitHub Pages feature, transforming molecular data from a spreadsheet into an interactive website accessible to the public.

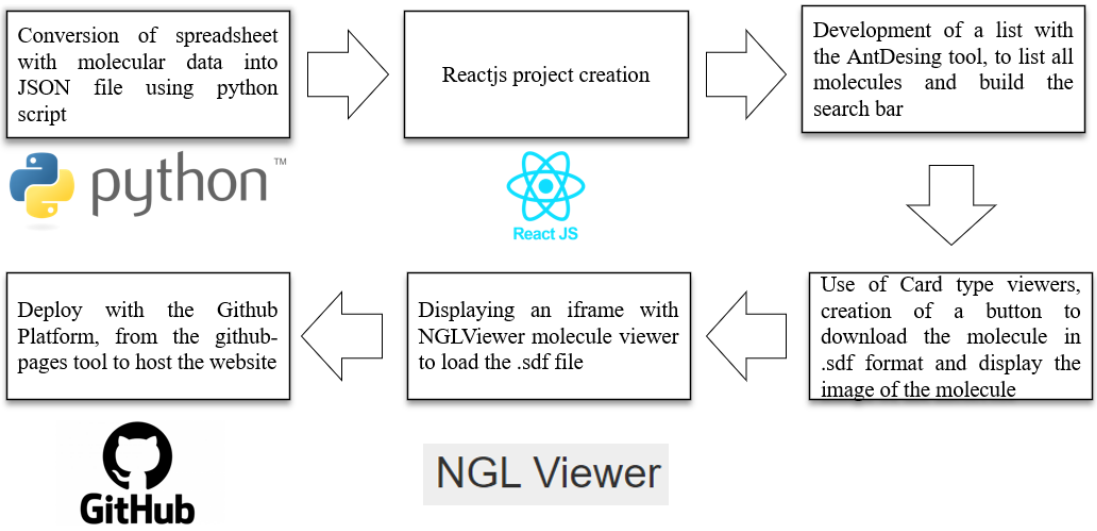


Fig. 3: Website development process.

4 LMW Database Applications

With the completion of the Human Genome Project and advancements in techniques such as protein purification and crystallography, computer science has become a fundamental element in drug discovery. In this scenario, Virtual Screening (VS) emerges as a more direct and economical method to identify potential drug candidates than traditional high-throughput experimental screening.

Virtual screening methods can be ligand-based or structure-based depending on the available information. When protein-target structure information is unavailable, ligand-based techniques, such as pharmacophore modeling and QSAR, are helpful. When protein-target structure information is available, structure-based drug design tools are used, including:

- Molecular Docking: This method predicts the orientation of a small molecule (such as a potential drug) when bound to a target protein to form a stable complex. Using molecular databases, it can be used to identify promising compounds. These compounds can be selected for further development and applications in drug discovery. [10].
- Molecular Dynamics: Molecular dynamics is a simulation technique that predicts the behaviour of molecules over time, typically used following molecular docking. These simulations can provide important insights into how a potential drug may interact with its target protein, such as the stability of the drug-protein complex and any conformational changes that may occur due to binding. [11].
- ADMET (Absorption, Distribution, Metabolism, Excretion, and Toxicity) predictions: Before a potential drug can be approved for use in humans, it is crucial to understand how it will be absorbed by the body, distributed to target tissues, metabolized, and excreted, as well as any potential toxicity that the compounds in

the database may possess. Using computational tools applied to the compounds in the LMW database we can make ADMET predictions that may help in the identification of compounds with a more favourable ADMET profile, saving time and resources. [12].

In the context of drug discovery, the use of databases is fundamental, as structured and molecular information can be an essential tool in this process. It allows for the storage, organization, and quick access of active ligand information, providing critical data for VS methods and molecular docking. These databases facilitate identifying and evaluating potential drug candidates, making pharmaceutical research more efficient and effective [10] [7].

In summary, a well-designed and implemented database with molecular information can be a powerful tool in drug design studies, facilitating the identification and evaluation of promising drug candidates for the applications mentioned.

4.1 Conclusion and Future Perspectives

In conclusion, creating a specific database for medicinal compounds derived from mushrooms can become a valuable tool in drug discovery. This database would allow quick and efficient access to diverse compounds, optimizing the virtual screening process and enabling the agile identification of compounds with therapeutic potential.

From a future perspective, expanding this database to include compounds from other sources such as marine fungi, other fungi, and plants like the fig tree would be a significant advancement. This expansion would increase the diversity and scope of the database, enabling the exploration of an even more comprehensive range of compounds with potential medicinal applications.

Therefore, investing in databases like this can accelerate the discovery of new drugs and open new avenues for studying natural compounds and their potential therapeutic applications.

References

1. ICFR Ferreira, JA Vaz, MH Vasconcelos, and A Martins. Compounds from wild mushrooms with antitumor potential. anticancer agents med chem 10: 424–436, 2010.
2. Carlos Seiti Hurtado Shiraishi. *Estudo do Potencial Anti-inflamatório de Uma Biblioteca de Compostos Naturais de Cogumelos por Screening Virtual Contra as Enzimas Cox (-1 E-2)*. PhD thesis, Instituto Politecnico de Braganca (Portugal), 2020.
3. Oludemi Taofiq, Ricardo C Calhelha, Sandrina Heleno, Lillian Barros, Anabela Martins, Celestino Santos-Buelga, Maria João RP Queiroz, and Isabel CFR Ferreira. The contribution of phenolic acids to the anti-inflammatory activity of mushrooms: Screening in phenolic extracts, individual parent molecules and synthesized glucuronated and methylated derivatives. *Food Research International*, 76:821–827, 2015.
4. Sunghwan Kim, Paul A Thiessen, Evan E Bolton, Jie Chen, Gang Fu, Asta Gindulyte, Lianyi Han, Jane He, Siqian He, Benjamin A Shoemaker, et al. Pubchem substance and compound databases. *Nucleic acids research*, 44(D1):D1202–D1213, 2016.
5. Anna Gaulton, Louisa J Bellis, A Patricia Bento, Jon Chambers, Mark Davies, Anne Hersey, Yvonne Light, Shaun McGlinchey, David Michalovich, Bissan Al-Lazikani, et al. Chembl: a large-scale bioactivity database for drug discovery. *Nucleic acids research*, 40(D1):D1100–D1107, 2012.
6. John J Irwin and Brian K Shoichet. Zinc- a free database of commercially available compounds for virtual screening. *Journal of chemical information and modeling*, 45(1):177–182, 2005.

7. Maria Sorokina, Peter Merseburger, Kohulan Rajan, Mehmet Aziz Yirik, and Christoph Steinbeck. Coconut online: collection of open natural products database. *Journal of Cheminformatics*, 13(1):1–13, 2021.
8. Noel M O'Boyle, Michael Banck, Craig A James, Chris Morley, Tim Vandermeersch, and Geoffrey R Hutchison. Open babel: An open chemical toolbox. *Journal of cheminformatics*, 3(1):1–14, 2011.
9. Thomas Sander, Joel Freyss, Modest von Korff, and Christian Rufener. Datawarrior: an open-source program for chemistry aware data visualization and analysis. *Journal of chemical information and modeling*, 55(2):460–473, 2015.
10. Xuan-Yu Meng, Hong-Xing Zhang, Mihaly Mezei, and Meng Cui. Molecular docking: a powerful approach for structure-based drug discovery. *Current computer-aided drug design*, 7(2):146–157, 2011.
11. Mitsugu Araki, Shigeyuki Matsumoto, Gert-Jan Bekker, Yuta Isaka, Yukari Sagae, Narutoshi Kamiya, and Yasushi Okuno. Exploring ligand binding pathways on proteins using hypersound-accelerated molecular dynamics. *Nature Communications*, 12(1):2793, 2021.
12. Nour El-Huda Daoud, Pobitra Borah, Pran K Deb, Katharigatta N Venugopala, Wafa Hourani, Muhammed Alzweiri, Sanaa K Bardaweel, and Vinod Tiwari. Admet profiling in drug discovery and development: perspectives of in silico, in vitro and integrated approaches. *Current Drug Metabolism*, 22(7):503–522, 2021.

Assessing Cybersecurity Risks in BLE-based Asset Management Systems

David Verde[1], Sara Paiva[1], and Sergio Lopes[1,2]

[1] ADiT-Lab, Instituto Politécnico de Viana do Castelo, Portugal
davidverde@ipvc.pt, sara.paiva@estg.ipvc.pt
[2] CiTin - Centro de Interface Tecnológico Industrial, Inovarcos, Portugal
sil@estg.ipvc.pt

Abstract. In the current era of digital transformation, asset management systems using beacons are being applied across various domains, allowing for the detection of individuals or objects within a building. While the impact of a compromised system may not be significant in certain domains, in others it can pose risks and potentially lead to the loss of human lives or other significant consequences. This paper presents a risk assessment of cyber-attacks targeting Bluetooth Low Energy (BLE) devices in two specific scenarios: healthcare and industry. The aim is to estimate the attacks that pose the greatest risk in each application area. Results show that risk levels vary depending on the targeted scenario. Replay, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks are the ones that pose the greatest risk levels in the considered scenarios.

Keywords: Indoor-Location Security · Asset Management · BLE Beacons · Bluetooth · Cybersecurity.

1 Introduction

Cybersecurity is an increasingly important topic in today's world, with cyberattacks on the rise [1, 2]. To contradict this growth, there is a need for increased research and protection of cyber systems, especially the most critical ones, to prevent future breaches [3]. BLE beacons are small-size, low-cost, wireless transmitters. They emerged as a solution for asset management, keeping track of people and objects in indoor/outdoor locations with great accuracy, being one of the most used location technologies [4]. Nowadays, this technology is implemented in several application areas, such as Healthcare or Industrial Environments [5]. The widespread adoption of these systems has made them attractive targets for cyberattacks, highlighting the need to ensure their safety from unauthorized access. Compromising one of these systems can result in incorrect location data, which can have serious consequences depending on the application area. For instance, in industrial environments, even a minor delay caused by incorrect location data can result in significant profit losses, while in healthcare settings, such failures can impact the localization of critical life-support systems. This work is aimed at assessing cybersecurity risks in Asset Management Systems (AMS) that use Bluetooth Low Energy (BLE) technology. The study focuses on industrial and hospital environments, which have distinct characteristics and pose unique cybersecurity challenges. The remainder of this paper is structured as follows. Section 2 presents the revision of related works. Section 3 explains beacons technology key features. Section 4 presents two scenarios: healthcare and industry. Before the conclusions, section 5 presents the risk assessment of cyber-attacks for both scenarios.

2 Related work

With the evolution of Bluetooth technology and the constant growth of smartphone usage, the creation of sophisticated and more accurate real-time indoor-location systems became possible [6]. For example, BLE-based indoor-location systems do not go unnoticed, which makes them a target for cyber-attacks [7]. Authors in [8] present a cyber-attack survey for the security and privacy of BLE. They also present possible attack scenarios for different types of vulnerabilities, classify them according to their severity, and list possible mitigation techniques. In [9], authors introduce the security concern theme relative to Low Power Wireless networks (LPW) due to their specific security vulnerabilities targeting the used communication protocols. Authors highlight that exploiting these vulnerabilities can lead to Energy depletion attacks (EDA), which can quickly drain the device's battery power. Authors in [10] address and discuss several indoor positioning system technologies. Regarding the security of these systems, data privacy was again deeply mentioned. The authors concluded that data privacy achievement depends totally on the design of the indoor positioning system. In [11], authors mainly focus on providing a complete survey of indoor localization systems and technologies, one of which is the BLE technology. This article also addresses the security challenges entailed, such as location privacy issues, weak authentication mechanism issues, energy efficiency, and environmental radio noise which can be exploited. In [12] and [13], authors address several threats related to IoT. Mitigation defenses are also proposed. Authors highlight some of the most severe, yet easy to exploit, security and privacy threats: leakage of personally identifiable information; leakage of sensitive user information; and unauthorized execution of functions. BLE beacons are being increasingly used in smart city applications, as discussed by the authors in [14]. This growth also rises an attractive target to adversaries for social or economic reasons. In this study, a contextualization of different attack types against beacon systems is given. To make security evaluation and the corresponding protection easier, the necessary potential impact and potential defense mechanisms for various threats are described. In [15], authors say that secure location sensing has the potential to improve healthcare processes regarding security, efficiency, and safety. Further, in the study is proposed an application called Beacon+ that uses BLE technology with the iBeacon protocol. This application is secured against spoofing, temporal, and authentication attacks. Authors also assure that the application enables secure location sensing, such as real-time tracking of hospital assets.

3 Beacon Technology Contextualization

Beacon devices are small-size, wireless transmitters that use BLE technology to send radio signals to all nearby devices that are BLE-enabled. BLE is currently one of the most used proximity-based location technology for both indoor and outdoor environments. Basically, they connect and transmit information to nearby devices, making the location-based search easier and more accurate. Beacon devices are powered by an embedded battery, usually replaceable. Depending on the beacon type and its configurations the useful lifetime varies, the more transmission power the more energy

consumption, thus reduced lifetime. BLE uses ***L2CAP*** for data transmission services. The deployment and georeferencing of beacon devices in a specific environment is a critical step to ensure optimal system performance. BLE beacons consist of a central processing unit (CPU), a radio signal transmitter based on BLE technology, and batteries. They periodically broadcast their unique identifier and other data packets to nearby Bluetooth-compatible devices, as illustrated in Figure 1. This identifier is received by the in-range devices, which are usually mobile ones, and then it is possible to determine the location of a certain device/user.

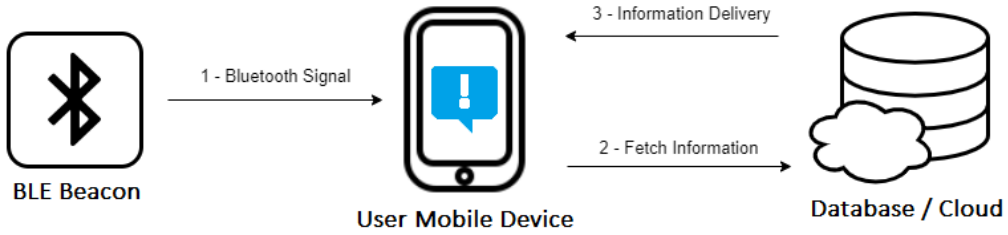


Fig. 1: Beacon Technology Architecture

The iBeacon protocol is based on BLE, being one of the most used for proximity-based positioning. It was developed by Apple, and originally targeted to iOS systems, but it also works on Android systems and every other compatible with BLE, since it uses Bluetooth 4.0 and Bluetooth 5.0 [16]. The iBeacon protocol has the following specifications:

- **Universally Unique Identifier (UUID):** a custom 16-byte number intended to identify the beacon;
- **Major:** a 2-byte number indented to identify the group within which the beacons are deployed (editable);
- **Minor:** a 2-byte number that identifies a subgroup within which the beacons have been deployed (editable);
- **Measured Power (TX Power):** The estimated received signal strength measured by a receiver that is positioned 1 meter away from the transmitter (editable);

4 Asset Management - Safety and Security

Asset management is a technique used to keep track of machinery, devices, or even human resources, depending on the application area. Next, two scenarios of asset management will be explained.

4.1 Industrial Scenario

Fig. 2 depicts an industrial scenario where machines are used autonomously to improve manufacturing productivity. For safety reasons, and to prevent workers from accidentally stepping into the operational zone of the machine, this use-case illustrates how an

indoor location system might be used to track staff members within the surrounding of the machine, being classified in two distinct zones Warning Zone and Danger Zone. This scenario follows the next workflow: 0) Each machine possesses two redundant beacons that are used in parallel to identify both zones. Also, staff members must be using one small wearable device that responds according to the information gathered from the beacons. 1) Supposing the distraction of a staff member, if he enters the Warning Zone (yellow area), his wearable device emits a signal, so the user remembers that he can not enter there and steps away, while the machine slows its working speed. 2) If the staff member continuously approaches the machine and enters the Danger Zone (red area), upon detection, the wearable device instantly emits a vibrating and sound signal to notify the user that he is crossing into the Danger Zone, while the machine stops completely. 3) The staff members get alerted and immediately leave the machine range area.

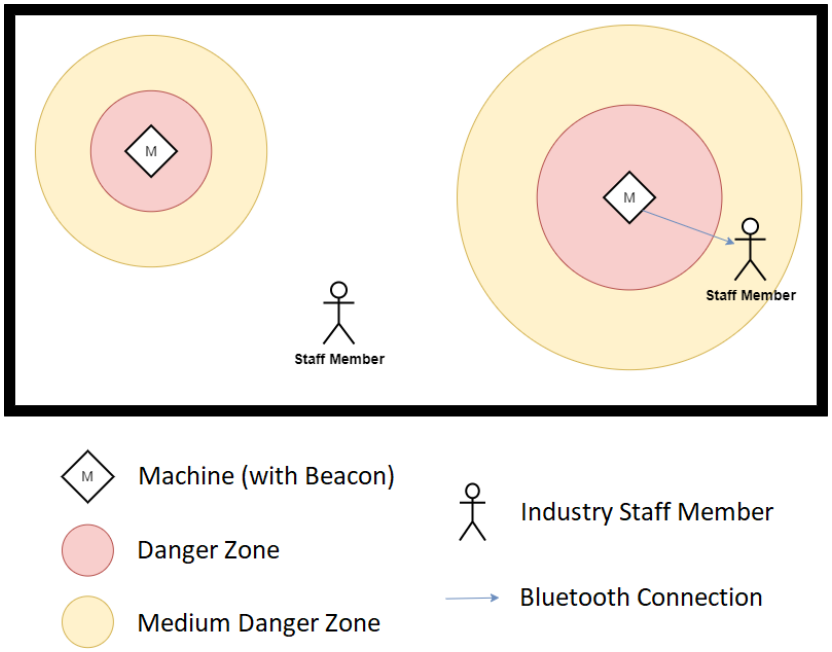


Fig. 2: Industrial Scenario

4.2 Hospital Scenario

In the hospital context, asset management is used to keep track of important machinery, nurses doctors, and even patients. Figure 3 presents a fictional hospital scenario created to simulate the real application of an indoor location system for hospitals. This scenario focuses on the quick location of needed health machines inside the hospital building, however, it can be applied to staff and patients' locations. This scenario follows the next workflow: 0) All hospital rooms are equipped with at least one BLE Beacon device and all the machinery is equipped with a Bluetooth receiver device that has an internet

connection; 1) The staff member situated in room 1 needs to fetch a specific health machine (that is in room 6), however, he does not know its location; 2) In room 6, the health machine device is receiving data from Beacon number 6, which identified that the machine is located at that room. Then, the device updates an online repository with the correct room through an internet connection; 3) The staff member uses an application previously installed on his mobile phone to check in which room the needed machine is, and gets the response that it is in room 6; 4) The staff member goes directly to room 6 and picks up the wanted health machine.

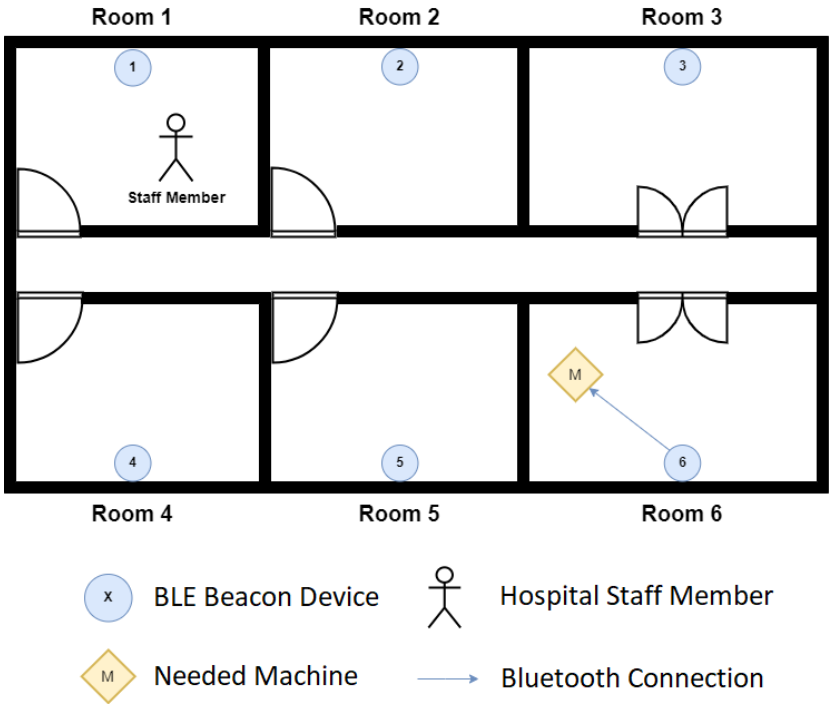


Fig. 3: Hospital Scenario

5 Cyber-Attacks and Risk Assessment

In this section, already discovered cyber-attacks that target BLE systems are presented. Based on the attacks found, and the scenarios presented in Section 4, a risk assessment was estimated, that considers the likelihood of happening and the impact of the attack. The probability scale of the attack happening is depicted in Table 1, which considers the difficulty of physical and digital access as the main factors. It was considered that anyone with access to both indoor scenario environments could be a malicious actor.

Taking into consideration the probability and impact scales, Table 3 presents the complete risk assessment of each attack for both industry and hospital scenarios. The impact scale of the attacks is depicted in Table 2. Individual safety, data privacy, and

Table 1: Probability Scale of Attack Occurrence

Level	Scale	Description
1	Rare	Requires physical access and device's authentication.
2	Possible	Requires proximity access and device's authentication.
3	Common	Requires device's authentication.
4	Likely	Requires proximity access.
5	Very likely	Requires physical access to the device.

work productivity were considered, in the respective order of priority. Risk is acknowledged as identifying the likelihood and seriousness of any potential harm in a given context. This risk assessment was carried out in order to identify the most hazardous attacks for the given scenarios and lately harden these systems.

Table 2: Impact Scale

Level	Scale	Description
1	Low	Reduced work rithm.
2	Moderate	Device's privacy compromised.
3	Major	Worker privacy compromised.
4	Extreme	Irreversible damages or even death of a pacient/worker.

The risk values presented in column *Risk* were calculated using the equation below (1), which multiplies the probability value by the impact value:

$$Risk = Probability \times Impact \tag{1}$$

The risk values could vary from 1 to 20, the more valuable the higher the risk level, being considered the following scale: from 1 to 4 low risk (light green), from 5 to 9 moderate risk (yellow), from 10 to 14 major risk (orange), and from 15 to 20 extreme risk (red).

As can be observed, some attacks have different risk levels depending on the target scenario, for example, the replay attack, which has extreme risk in the hospital scenario but low risk in the industry scenario. The replay, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks entail greater risk levels for the given scenarios.

Table 3: Cyber-Attacks and Risk Assessment

ID	Attack Title	Attack Description	Risk Assessment						Refs.
			Industry			Healthcare			
			Probability	Impact	Risk	Probability	Impact	Risk	
#1	Passive Sniffing Attack	The attacker places in the path of data transmission which allows him to eavesdrop and capture every data being transmitted. Most BLE devices have poor encryption functions which enable the attacker to decrypt the communication quite easily.	4	3	12	4	2	8	[17], [10], [18], [19], [20]
#2	Active MITM Attack	MITM stands for Man In The Middle. The attacker interferes with the communication process, corrupting the integrity of data. Intercepting data packages sent by one device, modifying and then sending it to other devices.	2	4	8	2	4	8	[10], [18], [21], [8]
#3	Replay Attack	The attacker captures data packets and re-transmits them with malicious intentions. Encrypted packets can also be re-transmitted if proper defense mechanisms are not implemented.	4	1	4	4	4	16	[17], [18], [19], [8]
#4	MAC Spoofing Attack	The attacker spoofs its MAC address pretending to be another device. Spoofing a MAC address is not a severe problem. However, when combined with other attacks, such as authentication attacks or DoS, can greatly increase the integrity and availability effectiveness.	4	1	4	4	1	4	[18], [21], [20], [22], [8]
#5	PIN Cracking Attack	This a type of cryptographic attack. The attacker captures packets sent by BLE devices and then tries to crack the key used in data encryption.	3	3	9	3	2	6	[17], [10], [21]
#6	Authentication Attack	The attacker tries to exploit the cryptographic weakness of BLE pairing process by observing the key exchanging and connection authentication process. Then, tries to recalculate the shared key for himself.	2	3	6	2	2	4	[17], [10], [23], [19], [20]
#7	Battery Exhaustion Attack	One of the main features of BLE is their low power consumption. An attacker can prevent the target device from entering into low-power mode, for example by making multiple fast connections, and drain its battery.	4	4	16	4	4	16	[9], [20], [8]
#8	Jamming Attack	This attack is a type of DoS and happens in the physical layer when an attacker sends needless signal through the communication channel creating radio noise between the connected devices.	4	4	16	4	4	16	[24], [21], [20], [22]
#9	Fuzzing Attack	The attacker uses a certain program to send corrupt random data or previously crafted malformed data to the target device which can make it crash or misbehave.	4	4	16	4	4	16	[24], [21], [20], [22]
#10	Blue-Smack Attack	BLE uses L2CAP for data transmission services. The attacker targets L2CAP protocol and disrupts the service. Similar to the Ping of Death attack.	4	4	16	4	4	16	[21], [21], [20]
#11	Device Fingerprinting Attack	This is an attack that tries to identify a device's unique features such as MAC address, UUID, GATT, and advertisement packets. Resumes in violation of privacy. Used to plan further attacks.	4	3	12	4	2	8	[10], [21], [20]
#12	Activity Detection Attack	This attack has the goal of tracking a user, without his consent, in a certain environment. The attacker can get confidential information by observing the BLE smart wearable (used in industry and health areas).	2	3	6	2	2	4	[10], [21], [20]
#13	Hijacking	Hijacking involves an unauthorized malicious actor gaining access to the configuration layer of the BLE device. This allows him to control the operational settings of a beacon device, including the UUID, major, minor, and transmission power.	3	4	12	3	4	12	[25], [26], [27], [8]

6 Conclusions

In this paper, an estimated risk assessment was presented co-relating the possible BLE cyber-attacks and two defined scenarios. It was concluded that the risk levels vary depending on the target scenario, for the same attack. The replay, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks imply increased risk levels for the given scenarios. As future work, the two created scenarios will be replicated so the higher-risk attacks can be exploited to present new mitigation defenses.

References

1. Marwan Albahar. Cyber attacks and terrorism: a twenty-first century conundrum. *Science and engineering ethics*, 25(4):993–1006, 2019.
2. Sanjana Sharma. Cyber security for the defence industry. *Cyber Security Review, online at http://www. cybersecurity-review. com/industry-perspective/cybersecurity-for-the-defence-industry*, 2017.

3. Mohammad Ghiasi, Moslem Dehghani, Taher Niknam, and Abdollah Kavousi-Fard. Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system. *Network*, 1(1), 2020.
4. Joakim Lindh. Bluetooth low energy beacons. *Texas Instruments*, page 2, 2015.
5. Pavel Kriz, Filip Maly, and Tomas Kozel. Improving indoor localization using bluetooth low energy beacons. *Mobile information systems*, 2016, 2016.
6. David Verde, Luís Romero, Pedro Miguel Faria, and Sara Paiva. Architecture for museums location-based content delivery using augmented reality and beacons. In *2022 IEEE International Smart Cities Conference (ISC2)*, pages 1–6, 2022.
7. Sungil Kim, Sunhwa Ha, Alshihri Saad, and Juho Kim. Indoor positioning system techniques and security. In *2015 Forth International Conference on e-Technologies and Networks for Development (ICeND)*, pages 1–4. IEEE, 2015.
8. Arup Barua, Md Abdullah Al Alamin, Md. Shohrab Hossain, and Ekram Hossain. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, 3:251–281, 2022.
9. Van-Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang. Energy depletion attacks in low power wireless networks. *IEEE Access*, 7:51915–51932, 2019.
10. PSP Ray Bernard. Indoor positioning systems.
11. Faheem Zafari, Athanasios Gkelias, and Kin K. Leung. A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3):2568–2599, 2019.
12. Constantinos Kolias, Angelos Stavrou, Jeffrey Voas, Irena Bojanova, and Richard Kuhn. Learning internet-of-things security "hands-on". IEEE Security & Privacy, 14(1):37–46, 2016.
13. Paul D Martin et al. *Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare*. PhD thesis, Johns Hopkins University, 2016.
14. Aldar CF Chan and Raymond MH Chung. Security and privacy of wireless beacon systems. *arXiv preprint arXiv:2107.05868*, 2021.
15. Paul D. Martin, Michael Rushanan, Thomas Tantillo, Christoph U. Lehmann, and Aviel D. Rubin. Applications of secure location sensing in healthcare. In *Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*, BCB '16, page 58–67, New York, NY, USA, 2016. Association for Computing Machinery.
16. Michael Wang and Jack Brassil. Managing large scale, ultra-dense beacon deployments in smart campuses. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 606–611. IEEE, 2015.
17. Shahin Farahani. *ZigBee wireless networks and transceivers*. newnes, 2011.
18. Sheeraz Kirmani, Abdul Mazid, Irfan Ahmad Khan, and Manaullah Abid. A survey on iot-enabled smart grids: Technologies, architectures, applications, and challenges. *Sustainability*, 15(1):717, 2023.
19. Michael A Rushanan. *An Empirical Analysis of Security and Privacy in Health and Medical Systems*. PhD thesis, Johns Hopkins University, 2016.
20. Dung Ho. Enterprise iot device visibility. 2021.
21. Sherali Zeadally, Farhan Siddiqui, and Zubair Baig. 25 years of bluetooth technology. *Future Internet*, 11(9), 2019.
22. Jennifer Ann Janesko. Bluetooth low energy security analysis framework, 2018.
23. Nasim Donyagard Vahed. Analysis of iot security weaknesses and ways to protect against them. 2020.
24. Qingchun Ren. *Medium access control (MAC) layer design and data query processing for wireless sensor networks*. The University of Texas at Arlington, 2007.
25. Hui Jun Tay, Jiaqi Tan, and Priya Narasimhan. A survey of security vulnerabilities in bluetooth low energy beacons. *Carnegie Mellon University Parallel Data Lab Technical Report CMU-PDL-16-109*, 2016.
26. Constantinos Kolias, Lucas Copi, Fengwei Zhang, and Angelos Stavrou. Breaking ble beacons for fun but mostly profit. In *Proceedings of the 10th European Workshop on Systems Security*, pages 1–6, 2017.
27. Mohammed Zubair, Devrim Unal, Abdulla Al-Ali, and Abdullatif Shikfa. Exploiting bluetooth vulnerabilities in e-health iot devices. In *Proceedings of the 3rd international conference on future networks and distributed systems*, pages 1–7, 2019.

A Survey and Risk Assessment on Virtual and Augmented Reality Cyberattacks

Tânia Silva[1,2], Sara Paiva[1,3], Pedro Pinto[1,5], and António Pinto[4,5]

[1] ADiT-Lab, Instituto Politécnico de Viana do Castelo, Viana do Castelo, Portugal
stania@ipvc.pt, sara.paiva@estg.ipvc.pt, pedropinto@estg.ipvc.pt
[2] Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, 5300-253 Bragança, Portugal
[3] ALGORITMI Research Center / LASI, University of Minho, Guimarães, Portugal
[4] CIICESI, ESTG, Instituto Politécnico do Porto, Portugal
apinto@estg.ipp.pt
[5] INESC TEC, Porto, Portugal

Abstract. Nowadays, Virtual Reality (VR) and Augmented Reality (AR) systems are not exclusively associated with the gaming industry. Their potential is also useful for other business areas such as healthcare, automotive, and educational domains. Companies need to accompany technological advances and enhance their business processes and thus, the adoption of VR or AR technologies could be advantageous in reducing resource usage or improving the overall efficiency of processes. However, before implementing these technologies, companies must be aware of potential cyberattacks and security risks to which these systems are subject. This study presents a survey of attacks related to VR and AR scenarios and their risk assessment when considering healthcare, automation, education, and gaming industries. The main goal is to make companies aware of the possible cyberattacks that can affect the devices and their impact on their business domain.

Keywords: Virtual Reality · Augmented Reality · Cyberattacks · Vulnerabilities · Risk Assessment

1 Introduction

Virtual Reality (VR) systems are used to create a virtual environment, which can either be a simulation of the real or a fictional world, where the user can interact with its components. During the experience, the user is completely immersed in the virtual world losing the perspective of the real one [1]. On the other hand, in Augmented Reality (AR) systems, the user does not lose the real-world perspective since virtually computed objects are integrated into the user's worldview [2]. Mixed Reality (MR) is a combination of VR and AR specifications. It complements the real world where the user can interact with virtual components displayed over his view [3].

The use of Virtual and Augmented Reality systems is highly associated with the gaming industry. However, over the years and due to its potential, it has been applied in other areas of business such as healthcare, the automotive industry, and education [4, 5]. According to *Finances Online*[1], in 2022, the Virtual and Augmented reality systems were considered more useful in the gaming industry, achieving a 61% score in utility. Healthcare, education and manufacturing, and automotive industries also achieved relevant scores of 41%, 41%, and 23% in utility, respectively.

[1] https://financesonline.com/virtual-reality-statistics/

The implementation of new technology requires additional considerations with respect to the existence of security flaws and how these can affect the final users. A security flaw that impacts systems mainly used in the gaming sector may not be as critical as if it affects devices used in healthcare. In healthcare, the impacts can cause significant damage to the users, since it is applied to individuals who are physically or psychologically more vulnerable.

This study presents a survey of attacks related to VR and AR scenarios and their impact on different domains of application. A risk assessment considering the probability and the impact was also developed and analyzed to determine the real risk that each attack brings to a specific domain. The result of the work herein can help develop future products by making them aware of potential cyberattacks and security risks, guiding these developments in producing better products.

The paper is organized as follows. Section 2 presents the documented attacks regarding Virtual and Augmented Reality systems. The four domains of application of VR and AR systems are presented in Section 3. Section 4 presents a discussion of the risk assessment results. The last section presents the main conclusions and future work.

2 Identified Cyberattacks

The attacks described in this section are the result of a systematic review, loosely based on the PRISMA methodology, that consisted in searching the Google Scholar and IEEE Xplore databases for the terms "Attack" OR "Vulnerability" AND "Virtual Reality" OR "Augmented Reality". Two survey papers were identified [6,7]. Additionally, 31 papers were collected and analysed. From this literature review, 15 attacks were identified and are presented next.

- **Chaperone:** consists in manipulating the VR walls to make the virtual space appear larger or smaller and, with these alterations, make the user lose perception of the real space [8,9].
- **Disorientation:** consists of a malicious modification of a virtual environment with the intention of causing physical or psychological harm to the user [8].
- **Overlay:** consists of overlaying persistent images and video content onto the user's view [8].
- **Human Joystick:** consists in controlling the user's movements in order to guide him to a predefined physical location without his perception [8].
- **Denial of Service:** consists of performing an overwhelming number of requests so that the system becomes unresponsive [9–14].
- **Unauthorized access:** consists in accessing a system or information without permission or consent [9,10,13].
- **Eavesdropping:** consists in intercepting information in a communication between two devices [10,14–22].
- **Observation or Shoulder-Surfing:** consist in observing the user behaviour to collect information, especially authentication information or other important information [13,19–21,23–27].
- **Tampering:** consists in modifying the components of the system in order to make them operate accordingly to the objective of the attacker [9,13].

- **Impersonation:** consists of a phishing attack where the malicious individual impersonates another person or organization to obtain confidential information [9, 14, 19, 27].
- **Run malicious code:** consists of the attacker making the system execute his code, with malicious intent [11, 12, 28–30].
- **Side-channel:** consists in extracting information not directly from the target system but from the observation of its characteristics while operating [16, 26, 27].
- **Hijacking:** consists in gaining unauthorized access to a system by intercepting a communication, by predicting or stealing a session token [17, 19, 31].
- **Jamming:** consists of interfering with the communication channel to perturb the system functionality [32].
- **Ransomware:** consist in encrypting information making them inaccessible to the user [29].

The first four attacks apply specifically to Virtual Reality Systems.

3 Domains of application

For the context of this work, four domains were chosen that might benefit from the implementation of VR and AR systems. The domain choice relies on the analysis made by the *Finances Online* that identifies the gaming, healthcare, automotive industry, and education domains as those that profit the most from the implementation of VR and AR technologies. In a common gaming domain, the user buys a headset and enjoys the immersive experience in the safety of his home where the network is private and only authorized people can establish a connection to the network. In the healthcare domain, VR/AR systems are used in a therapeutic context. The headsets simulate an environment adapted for a specific therapy or treatment [33]. While the patient is performing the requested tasks, a professional is monitoring his performance. The sessions are carried out in a health institution where the network is private. In the automotive industry, these technologies are used to train new employees in an efficient way that leads to cost reduction. The trainee uses the headset to have a guide on how to perform a vehicle repair. This technique discards the usage of actual equipment and reduces the need to have a professional technician with the trainee. The network is also private in the industrial domain [34]. Finally, these VR and AR systems are also used to enhance the student's experience in classes. They can be used to obtain more information about a monument or to explain how the digestive system works. For this domain, students use headsets to access a multiplayer educational environment where they can learn and interact with each other. The teacher can manage and have feedback on the tasks performed. The network in the institution is public [35].

4 Risk Assessment

This section presents a risk assessment considering the probability of an attack happening and the impact that a successful attempt can bring to the company or individual. The main goal is to clarify the risk that each attack, collected in section 2, may have in

Table 1: Probability scale

Level	Scale	Description
1	Rare	Requires physical access to devices or locations. The attacker has full access to the devices and locations.
2	Possible	Requires physical and authenticated access to devices and locations. The attacker has unauthenticated access to the devices.
3	Common	Requires attackers to be in the vicinity of devices or locations. The attacker is able to convince the user to install malicious software.
4	Likely	Requires devices or locations to be connected to the internet, but only allows authenticated connections. The attacker has the capability to install software remotely with user intervention.
5	Very likely	Requires devices or locations to be connected to the internet. The attacker has the capability to install software remotely without user intervention.

Table 2: Impact scale

Level	Scale	Individual Safety	Organization reputation
1	Very low	Causes insignificant injuries, no need for medical assistance.	Causes insignificant damage which does not affect the organization's operation and reputation.
2	Low	Causes insignificant injuries that are easily treated with medical assistance.	Causes low-cost damage without affecting the organization's reputation.
3	Moderate	Causes significant injuries that are reversible with the user's hospitalization.	Causes reversible damage that affects the organization's reputation.
4	Major	Causes permanent injuries that require the user's hospitalization.	Causes permanent damage that denigrates the organization's reputation.
5	Extreme	Causes the user's death.	Causes the organization's bankruptcy.

the different domains. Equation (1) depicts the risk formula considered for this study, heavily based on ISO 27005 methodology [36].

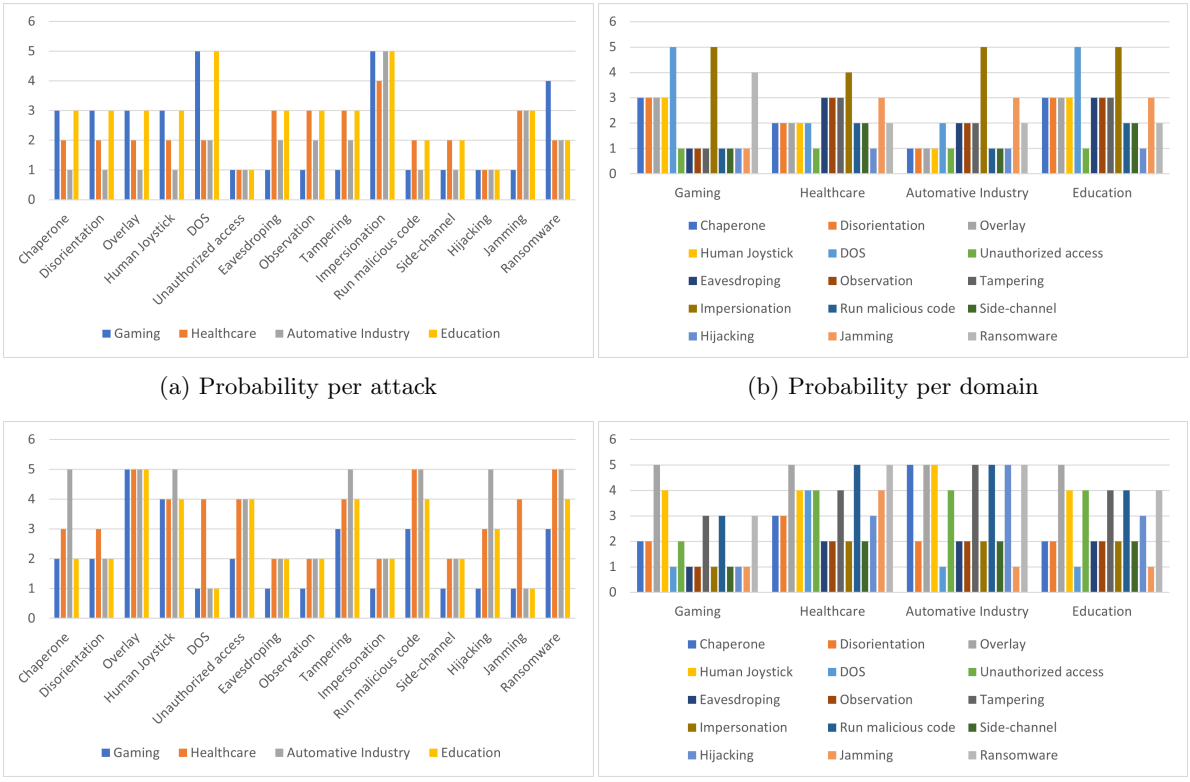
$$Risk = Probability \times Impact \tag{1}$$

The probability scale, shown in Table 1, varies between *Rare* and *Very likely* to happen. This classification ponders aspects such as physical and remote access to the locations or devices and their authentication methods. The impact scale, shown in Table 2, varies between *Very low* and *Extreme*. This classification contemplates individual safety and the organization's reputation. Therefore, the attack's purpose can either be directed to a user or to a company, at different levels.

Figures 1a), 1b), 1c) and 1d) depict the Probability and Impact classifications for each attack in the gaming, healthcare, automotive industry, and education domains.

4.1 Probability classification

Analyzing Figure 1a) one can conclude that the probability differs per domain. It is necessary to install malicious code into devices to perform Chaperone, Disorientation,



(a) Probability per attack

(b) Probability per domain

(c) Impact per attack

(d) Impact per domain

Fig. 1: Impact and Probability values per Attack and per Domain

Overlay, and Human Joystick attacks. In the Gaming and Educational domains it is necessary to access the Internet to carry out the tasks, being easier for the attacker to convince the targets to install the malicious code. Accordingly, a level 3 of probability was attributed to this domain. However, in the healthcare and automotive domains, the devices do not need to be connected to the network which decreases the probability level. The attacker goes unnoticed in a healthcare environment since it is a public space that receives thousands of people every day. Thus, it was assigned a level 2 of probability. In the automotive scenario, the entrances are more controlled so the probability lowers to level 1. In the gaming industry, the Denial of Service (DoS), Impersonation, and Ransomware attacks are more likely to happen due to the characteristics of the gaming environment, requiring devices to be connected to the internet to download or play the games. This user becomes a better target for the attacker that can perform remote attacks. In the Healthcare domain, Eavesdropping, Observation, Tampering, Impersonation, and Jamming attacks have more probability of occurring due to the quantity of non-identified persons that can enter the building and try to connect to the network unnoticed. The automotive industry is a more restrictive environment. Only authorized people have access to locations and the internet. Impersonation and Jamming are the most common attacks due to business competitors who aspire to affect the business process. Similar to the gaming industry, in the educational environment

Table 3: Risk analysis

Attack	Papers	Headset	VR/AR/MR	Risk				Intention
				G	H	A	E	
Chaperone	[8, 9]	HTC Vive	VR	6	6	5	6	Harm or disturb
Disorientation	[8]	HTC Vive	VR	6	6	2	6	Harm or disturb
Overlay	[8]	HTC Vive	VR	15	10	5	15	Harm or disturb, Manipulate
Human Joystick	[8]	HTC Vive	VR	12	8	5	12	Harm or disturb, Manipulate
DOS	[9–14]	HTC Vive	AR/VR/MR	5	8	2	5	Harm or disturb
Unauthorized access	[9, 10, 13]	HTC Vive	AR/VR/MR	2	4	4	4	Obtain information, Profit
Eavesdropping	[10, 14–22]	Google Cardboard, Oculus Quest and HTC Vive & Pro, HoloLens	AR/VR	1	6	4	6	Obtain information
Observation	[13, 19–21, 23–27]	All headsets	VR/AR/MR	1	6	4	6	Obtain information
Tampering	[9, 13]	HTC Vive	VR/MR	3	12	10	12	Obtain information, Manipulate, Profit
Impersonation	[9, 14, 19, 27]	HTC Vive	VR	5	8	10	10	Obtain information, Manipulate, Profit
Run malicious code	[11, 12, 28–30]	Oculus Quest	VR	3	10	5	8	Obtain information, Harm or disturb, Manipulate, Profit
Side-channel	[16, 26, 27]	Google Cardboard, Oculus Quest and HTC Vive Pro	VR	1	4	2	4	Obtain information
Hijacking	[17, 19, 31]	HTC Vive VR	VR/AR	1	3	5	3	Obtain information, Profit
Jamming	[32]	HTC Vive VR	VR	1	12	3	3	Harm or disturb
Ransomware	[29]	Oculus Quest 2	VR	12	10	10	8	Profit

DoS and Impersonation are the most probable attacks since the device needs to be connected to the network to enter the multiplayer environment. If significant confidential information can be collected about the user, it becomes a provable candidate for an impersonation attack.

Figure 1b) presents the probability classification from the attack perspective. Analyzing the Figure, it is visible that DoS, Impersonation, and Jamming are the most probable attacks. DoS and Impersonation are easily performed in devices with access to the internet and Jamming can be performed in any nearby devices with the intent of interfering with the system functionality, increasing the probability level for these attacks. The most affected are the Gaming and Education domains.

4.2 Impact classification

Figures 1c) and 1d) present the impact classification per domain and attack perspective, respectively. Analyzing Figure 1c), it is noticeable that the automotive industry is the most affected in case of cyberattacks followed by the healthcare, education, and gaming industries, respectively. This is due to the business competitors that can profit from stealing confidential information or affecting the organization's process. On the other hand, an attack with the intent of changing the virtual environment and its boundaries can cause serious injuries or even the death of the trainee working in a factory environment since they can enter a machine's danger zone.

In the healthcare industry, all the attacks have a significant impact. In a therapeutic context the virtual environment is designed for a specific treatment, even a small change in this domain can perturb or cause permanent damage to the patient. Attacks with the objective of collecting personal information or preventing the device's normal functionality have a high impact level. For example, a ransomware attack can encrypt all the devices in the hospital and make them unusable which would affect all the hospital processes from routine consults to important surgeries. In the educational domain, minors' confidential information is stored. A leak of this kind of information

would affect several families and degrade the institution's reputation. In the game industry, the most impactful attacks aim to harm or perturb the user. Attacks aiming to collect confidential information have a lower impact since the user may not have important information stored in the device. From the attack perspective, Figure 1d), Overlay attacks have an extreme impact in all the domains considering that is possible to generate continuous flashes that may trigger a seizure episode in persons with epilepsy. Human Joystick attack has also a high impact since the attacker is able to direct the user to an intended destination. Following these attacks, running malicious code and ransomware have more impact because a successful attack can compromise the industry's work process.

5 Risk classification

This subsection presents the risk classification of the surveyed attacks. Table 3 shows a risk analysis that, besides the computed total risk value per domain, also includes, per attacks, the targeted headset [6], the attack intention [7] and if its applicable to AR, VR or MR. Particularly, the objective of an attack can be to *harm* or mentally *disturb* the end user, to *manipulate* the user in believing or doing what the attacker intents, to *obtain confidential information* about the user or the company, to gain knowledge or to *profit*.

Table 3 shows that most of the attacks have a significant risk. Healthcare (H) and Education (E) are the most affected domains with higher risk values, on average. As expected, the Gaming (G) domain has a lower risk, on average, since most of the time it is performed in a controlled environment, the device may not contain personal information and even if the attack succeeds, it only affects one person. The Automotive (A) domain presents with a higher risk the tampering, impersonation, and ransomware. The overlay was the only attack with very high risk because it can harm any person with epilepsy. The side-channel attack has the lowest risk value.

6 Conclusions and Future Work

The work herein proposes two classifications for VR/AR cyberattack probability and impact estimation and performs a risk assessment of these attacks. A systematic review of the literature was conducted in order to collect the cyberattacks reported for VR/AR systems. The classification was performed for the domains in which these technologies are most useful, being gaming, healthcare, automotive and education industries, respectively. This study is a contribution for companies that intend to implement VR and AR technologies in their business processes making them aware of the security risks associated with different systems and devices. From the risk analysis, it is clear that one attack can have different impacts depending on the domain to which it is applied. In conclusion, Overlay, Human Joystick, and Tampering are the most dangerous attacks and Gaming and Educational are the most affected domains.

Future work involves the development of a proof of concept for some attacks using different VR or AR headsets to understand the impact on the end user. A definition

of mitigation methods for the identified attacks is also planned for the companies that have already implemented these technologies.

References

1. Oluleke Bamodu and Xu Ming Ye. Virtual reality and virtual reality system components. In *Advanced materials research*, volume 765, pages 1169–1172. Trans Tech Publ, 2013.
2. Julie Carmigniani and Borko Furht. *Augmented Reality: An Overview*, pages 3–46. Springer New York, New York, NY, 2011.
3. Mark Billinghurst and Hirokazu Kato. Collaborative mixed reality. In *Proceedings of the first international symposium on mixed reality*, pages 261–284, 1999.
4. Mohamed Adel Mahmoud Abdelmaged. Implementation of virtual reality in healthcare, entertainment, tourism, education, and retail sectors. 2021.
5. Ronald T. Azuma. A Survey of Augmented Reality. *Presence: Teleoperators and Virtual Environments*, 6(4):355–385, 08 1997.
6. Abrar Alismail, Esra Altulaihan, M. M. Hafizur Rahman, and Abu Sufian. A systematic literature review on cybersecurity threats of virtual reality (vr) and augmented reality (ar). In I. Jeena Jacob, Selvanayaki Kolandapalayam Shanmugam, and Ivan Izonin, editors, *Data Intelligence and Cognitive Informatics*, pages 761–774, Singapore, 2023. Springer Nature Singapore.
7. Blessing Odeleye, George Loukas, Ryan Heartfield, Georgia Sakellari, Emmanouil Panaousis, and Fotios Spyridonis. Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers & Security*, 124:102951, 2023.
8. Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing*, 18(2):550–562, 2021.
9. Samaikya Valluripally, Aniket Gulhane, Reshmi Mitra, Khaza Anuarul Hoque, and Prasad Calyam. Attack trees for security and privacy in social virtual reality learning environments. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–9, 2020.
10. Viraj Dissanayake. A review of cyber security risks in an augmented reality world. 10 2018.
11. Blessing Odeleye, George Loukas, Ryan Heartfield, and Fotios Spyridonis. Detecting framerate-oriented cyber attacks on user experience in virtual reality. 08 2021.
12. Samaikya Valluripally, Aniket Gulhane, Khaza Anuarul Hoque, and Prasad Calyam. Modeling and defense of social virtual reality attacks inducing cybersickness. *IEEE Transactions on Dependable and Secure Computing*, 19(6):4127–4144, 2022.
13. Sanskar Syal and Rejo Mathew. Threats faced by mixed reality and countermeasures. *Procedia Computer Science*, 171:2720–2728, 2020. Third International Conference on Computing and Network Communications (CoCoNet'19).
14. Aniket Gulhane, Akhil Vyas, Reshmi Mitra, Roland Oruche, Gabriela Hoefer, Samaikya Valluripally, Prasad Calyam, and Khaza Anuarul Hoque. Security, privacy and safety risk assessment for virtual reality learning environment applications. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–9, 2019.
15. Meet the man-in-the-room attack: Hackers can invisibly eavesdrop on Bigscreen VR users.
16. Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu. Face-mic: Inferring live speech and speaker identity via subtle facial dynamics captured by ar/vr motion sensors. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, MobiCom '21, page 478–490, New York, NY, USA, 2021. Association for Computing Machinery.
17. Ananya Yarramreddy, Peter Gromkowski, and Ibrahim Baggili. Forensic analysis of immersive virtual reality social applications: A primary account. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 186–196, 2018.
18. Shiqing Luo, Xinyu Hu, and Zhisheng Yan. Hologlogger: Keystroke inference on mixed reality head mounted displays. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 445–454, 2022.
19. Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M Redmiles. Ethics emerging: the story of privacy and security perceptions in virtual reality. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 427–442, 2018.
20. Ellysse Dick. Balancing user privacy and innovation in augmented and virtual reality. Technical report, Information Technology and Innovation Foundation, 2021.

21. Song Chen, Zupei Li, Fabrizio Dangelo, Chao Gao, and Xinwen Fu. A case study of security and privacy threats from augmented reality (ar). In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pages 442–446, 2018.
22. Kiron Lebeck, Tadayoshi Kohno, and Franziska Roesner. How to safely augment reality: Challenges and directions. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, page 45–50, New York, NY, USA, 2016. Association for Computing Machinery.
23. Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. *ACM Trans. Comput.-Hum. Interact.*, 28(1), jan 2021.
24. Karthik Viswanathan and Abbas Yazdinejad. Security considerations for virtual reality systems, 2022.
25. Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Comput. Surv.*, 52(6), oct 2019.
26. Zhen Ling, Zupei Li, Chen Chen, Junzhou Luo, Wei Yu, and Xinwen Fu. I know what you enter on gear vr. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 241–249, 2019.
27. Shiqing Luo, Anh Nguyen, Chen Song, Feng Lin, Wenyao Xu, and Zhisheng Yan. Oculock: Exploring human visual system for authentication in virtual reality head-mounted display. In *Network and Distributed System Security Symposium*, 2020.
28. Wen-Jie Tseng, Elise Bonnail, Mark McGill, Mohamed Khamis, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. The dark side of perceptual manipulations in virtual reality. In *CHI Conference on Human Factors in Computing Systems*. ACM, apr 2022.
29. Michael Mahan. Exploring ransomware on the oculus quest 2. 2022.
30. Franziska Roesner, Tadayoshi Kohno, and David Molnar. Augmented reality: challenges & opportunities for security and privacy. *J Comput Secur Neurosci—Part*, 1(2), 2021.
31. Stefano Baldassi, Tadayoshi Kohno, Franziska Roesner, and Moqian Tian. Challenges and new directions in augmented reality, computer security, and neuroscience – part 1: Risks to sensation and perception, 2018.
32. Muhammad Usman Rafique and Sen-ching S. Cheung. Tracking attacks on virtual reality systems. *IEEE Consumer Electronics Magazine*, 9(2):41–46, 2020.
33. Tarja Susi, Mikael Johannesson, and Per Backlund. Serious games: An overview. 2007.
34. Glyn Lawson, Davide Salanitri, and Brian Waterfield. Vr processes in the automotive industry. In *International Conference on Human-Computer Interaction*, pages 208–217. Springer, 2015.
35. Dani Blum. So what exactly is avantis world?
36. https://www.iso.org/standard/75281.html.

Vulnerabilities in Baseboard Management Controllers: Risks and Mitigation Strategies in the IIoT Environment

Jackson Júnior[1], Sérgio Ivan[1,2], and Pedro Pinto[1,3]

[1] ADiT-LAB, Instituto Politécnico de Viana do Castelo, IPVC, Portugal
jacksonjunior@ipvc.pt
[2] CiTin, Portugal
sil@estg.ipvc.pt
[3] INESC TEC, Portugal
pedropinto@estg.ipvc.pt

Abstract. Vulnerabilities in Baseboard Management Controllers (BMCs) have a high impact on the Industrial Internet of Things (IIoT) environment. Recently, a set of vulnerabilities in BMCs disclosed by Nozomi Networks expose Operational Technology (OT) and IIoT networks to remote attacks.
This paper reviews a set of vulnerabilities in BMC affecting IIoT devices and discusses the risks and implications of the vulnerabilities found, and how they can be mitigated.
The discovery of vulnerabilities in BMC highlights the urgent need for a comprehensive and multifaceted approach to securing the IIoT environment. It is concluded that a general improvement in the security of BMC could be achieved by adopting the open-source philosophy and standardizing the hardware interface.

Keywords: BMC (Baseboard Management Controller) · firmware vulnerabilities · IIoT (Industrial Internet of Things).

1 Introduction

The Industrial Internet of Things (IIoT) has revolutionized the way industrial systems operate, providing endless possibilities for connectivity and automation. However, with this, increased reliance on technology comes a need for robust security measures to protect against potential vulnerabilities and attacks.

Baseboard Management Controllers (BMCs) are specialized service processors traditionally found in server motherboards and used for remote monitoring and managing a host system, including performing low-level system operations such as firmware flashing and power control. However, in recent years, BMCs have also been used increasingly in devices Operational Technology (OT) and IIoT. While BMCs offer convenience through remote monitoring and management, they also present a broader attack surface and can increase the overall risk of a system if not adequately protected.

Recently, security company Nozomi Networks analyzed a BMC from Taiwanese vendor Lanner Electronics and uncovered 13 vulnerabilities that affect their IAC-AST2500A expansion card [1]. The firmware of the IAC-AST2500A [2] is based on the American Megatrends (AMI) MegaRAC SP-X solution [3], which is also used by major brands such as Asus, Dell, Gigabyte, HP, Lenovo, and nVidia [4].

This research aims to review the vulnerabilities discovered by Nozomi Networks in BMCs and to discuss the potential risks and consequences of these vulnerabilities on OT and IIoT networks. Additionally, it aims to provide recommendations for increasing

security and mitigating these vulnerabilities, specifically in devices utilizing the AMI MegaRAC SP-X solution [4].

The rest of the paper is organized as follows. Section 2, presents related work. Section 3 presents the results. Section 4 discusses the findings, implications, and how the vulnerabilities can be mitigated. Section 5 provides the conclusions and outlines the future research directions.

2 Related Works

In the field of Internet of Things (IoT) and IIoT security, several works have addressed the issue of detecting and preventing cyber attacks on connected devices. Karande et al. [5] presents a review of the state of the art of IoT security needs and implementation mechanisms and proposes a real-time security attack detection system using a Google cloud platform. The work demonstrates the experimental setup and performs a performance analysis of the proposed system. Xenofontos et al. [6] present a systematic review of IoT security from three major sectors: consumer, commercial, and industrial. The work provides definitions for each sector and discusses operational requirements, implicit security constraints, mission criticality, and potential outcomes in the event of a compromise targeting the respective IoT sectors.

In the field of BMC security, Latzo et a. [7] introduce a memory acquisition tool called BMCLeech to perform unobtrusive memory forensics on operating systems. The tool is based on a BMC and exploits the Direct Memory Access (DMA) capability of the host through the BMC. BMCLeech is capable of acquiring a system's memory unobtrusively, as it is a standard device on many systems, and the host, therefore, cannot distinguish between "good" activities (such as server administration) and "bad" activities (taking memory snapshots). Furthermore, BMCLeech is capable of transparently acquiring memory for the operating system, making it a viable option for the forensic analysis of operating systems.

Frazelle [8] discuss the various security concerns related to BMCs, including the fact that the stack Intelligent Platform Management Interface (IPMI) was not designed with security in mind and has a history of vulnerabilities. The work also highlights the issue of proprietary software and vulnerabilities in BMC itself, citing examples such as USBAnywhere and Pantsdown vulnerabilities. In addition, the paper discusses the BMC's access to host firmware via Serial Peripheral Interface (SPI) and host memory through DMA, making it a prime target for hackers. The lack of a secure boot in BMC firmwares is also a concern mentioned in the article. In general, the work emphasizes the importance of improving the security of BMCs, given its privileged access and critical role in the operation of the servers.

Frazelle [9] presents a comprehensive overview of the importance of secure booting mechanisms in ensuring hardware and software integrity in modern computing systems. The work discusses the concept of a hardware root of trust, which aims to verify that the software installed in all hardware components is the intended software. It also introduces the Trusted Platform Module (TPM), a standard for a microchip designed to secure hardware through cryptographic keys, and its role in attestation, which reports on the state of the hardware and software configuration to establish code identity to remote or

local verifiers. The paper also discusses the challenges of implementing a hardware root of trust, such as the lack of transparency in proprietary firmware and the need for open-source options. It concludes by stressing the importance of secure booting mechanisms in today's security landscape, given the increasing threat of supply chain attacks, evil maid attacks, and cloud provider vulnerabilities.

Farmer [10] presents an important work in the field of BMC security, which includes a scan of the IPMI protocol across the internet and identifies a high percentage of vulnerable BMCs that could be compromised through basic configuration and protocol weaknesses. The work highlights the security risks of BMCs, including vulnerabilities in the IPMI protocol and poor implementations by BMC manufacturers, and discusses the impact of these vulnerabilities on the security of servers and large-scale data centers that rely heavily on IPMI for management and deployment. The authors also argue that the widespread use of vulnerable BMCs will continue to be a problem for years to come due to the large number of servers that include them.

Despite the critical nature of the issue, the topic of BMCs security is just beginning to be discussed in academia. This study aims to contribute to this body of research by disseminating security vulnerabilities identified by the industry and proposing security recommendations to mitigate similar vulnerabilities in equipped devices IoT and IIoT.

3 Vulnerabilities in Baseboard Management Controllers

Nozomi Networks detected 13 vulnerabilities in Lanner Electronics BMCs. Among these, five are rated as 9 or higher on the Common Vulnerability Scoring System (CVSS), thereby indicating their high severity. These vulnerabilities include CVE-2021-26727, CVE-2021-26728, CVE-2021-26729, CVE-2021-26730, and CVE-2021-26731.

Apart from CVE-2021-26730, each of the vulnerabilities is categorized under Common Weakness Enumeration (CWE), CWE-787, and CWE-77, both of which are associated with code execution. *CWE*-787, also known as Out-of-bounds Write, is a type of vulnerability in which an application unintentionally writes data beyond the established boundary of a memory structure, such as a buffer or array [11]. *CWE*-77, designated as Improper Neutralization of Special Elements Used in a Command ('Command Injection'), describes a system weakness whereby an application or system may inadvertently allow user input to direct the execution of system commands or queries, without conducting adequate input validation or sanitization. They can be exploited through the "spx_restservice" web service, which is accessible through the web interface of the IAC-AST2500A expansion card.

The remaining 8 vulnerabilities found (CVE-2021-26732, CVE-2021-26733, CVE-2021-44776, CVE-2021-44467, CVE-2021-44769, CVE-2021-46279, CVE-2021-45925, CVE-2021-4228) are of medium or low severity.

The vulnerabilities related to CWE -862 (CVE-2021-26732, CVE-2021-26733, CVE-2021-44776) represent weaknesses in authorization, allowing unauthorized access to sensitive data or actions. Their exploitation can lead to altered network configurations, host disruption, and Cross-Site Scripting (XSS) attacks.

Further vulnerabilities include the capability for active session termination (CVE-2021-44467), Denial-of-Service (DoS) condition on BMC (CVE-2021-44769), session

hijacking (CVE-2021-46279), legitimate username discovery (CVE-2021-45925), and Man-in-the-Middle (MitM) attacks (CVE-2021-4228).

The criticality of these vulnerabilities and possible mitigation strategies are discussed in the following section.

4 Discussion

It is crucial to note that the potential impact of these vulnerabilities extends beyond financial concerns and encompasses significant risks to human lives, national security, and political stability. Previous incidents have highlighted the severity of these risks, with reported attacks on food manufacturers [12], water treatment facilities [13], and the oil industry [14] resulting in food shortages, the potential poisoning of thousands of people, and potential environmental disasters. The potential for a chain reaction of such incidents further emphasizes the urgency and gravity of addressing these vulnerabilities in industrial control systems and IIoT networks.

Firewall and Intrusion Prevention System (IPS) security solutions typically focus on blocking external threats at the perimeter level of a network, but they are not efficient in controlling or stopping the propagation of threats that have already breached the network [15]. Traditional measures, such as firewalls and IPS, used in isolation, are insufficient to mitigate the vulnerabilities presented in this research. Therefore, a multifaceted approach is necessary to address the vulnerabilities in BMCs that have been discussed in this investigation.

On the one hand, several steps can be taken to mitigate vulnerabilities in IIoT systems in their current context. This includes implementing a comprehensive security policy that focuses on raising awareness about the importance of IIoT devices, implementing a configuration management policy that includes regular firmware checks and updates, implementing multi-factor authentication methods, using password managers and physical cryptographic key tokens to enforce the use of strong passwords, and implementing network segmentation based on device attributes, service types, and network information to prevent the direct exposure of BMCs to the Internet and ensure secure connections with multi-factor authentication [16].

On the other hand, a general improvement in the security of BMCs can also be achieved by adopting the open-source philosophy. Projects such as OpenBMC and U-bmc, which use thread-safe programming languages and replace the vulnerable IPMI protocol with gRPC, provide a promising approach by promoting transparency and community-driven development. Furthermore, initiatives such as RunBMC, which standardizes the hardware interface for BMCs and allows isolation and locking of the subsystem, can also improve security by making it easier to replace or update BMCs and integrate additional security measures. By open-sourcing the software at the lowest levels of the stack, we can provide visibility into the code running with the most privileges on the systems. This approach will lead to more eyes scrutinizing the code, encourage more minimal architectures, and lessen the risk that systems are caught off guard in the future [8].

Evidently, these open-source and hardware standardization initiatives should consider measures such as not using pre-programmed passwords on IIoT devices, meaning

that all passwords must be unique and should not return to their original credentials state upon factory reset [17]. Furthermore, devices should have viable hardware security schemes, such as cryptographic processors, Physically Unclonable Functions (PUFs), Hash-based Message Authentication Codes (HMACs), and random key generators [18, 19]. These alternatives also make it cheaper for manufacturers to ensure long-term updates of this hardware and software.

The vulnerabilities discovered in Lanner Electronic's BMCs pose a significant threat not only to the security of IIoT and OT systems but also to human lives.

The industry must take a multifaceted approach to address these vulnerabilities, focusing on short-term mitigation strategies, such as network segregation and regular firmware updates, and long-term solutions, such as adopting open-source software and hardware development.

5 Conclusion

This research aimed to investigate and provide information on the potential vulnerabilities in BMCs and their impact on the environment IIoT. Specifically, we focused on the recent discovery of vulnerabilities in BMCs made by Nozomi Networks that can expose OT and IIoT networks to remote attacks.

In the discussion section, the implications of the vulnerabilities found and how they can be mitigated are presented. We highlighted that traditional measures such as firewalls and IPS, used in isolation, are insufficient to mitigate the vulnerabilities presented in this research. Consequently, a multifaceted approach is necessary to address the vulnerabilities in BMCs.

Therefore, it was suggested that a general improvement in the security of BMCs could be achieved by adopting the open source philosophy and standardizing the hardware interface, jointly by implementing a comprehensive security policy that focuses on raising awareness of the importance of IIoT devices, managing configuration that includes regular firmware checks and updates, multifactor authentication methods, and network segmentation based on device attributes, service types, and generated information.

It is important to note that this research is based on a specific discovery of vulnerabilities made by Nozomi Networks in a specific brand of BMCs. While the findings provide valuable information, it is crucial to understand that the vulnerabilities and risks discussed may not apply to other brands or models of BMCs. However, the security measures suggested in this research can provide general protection, as the vulnerabilities were classified into the categories of Service, Communication, and Device according to a taxonomy used as a reference.

Future developments of this research could involve investigating ways to make the use of cryptographic and authentication mechanisms on resources-limited IIoT devices viable, such as the use of cryptographic processors, PUFs, HMACs, and random key generators. This could involve exploring new techniques to secure these devices, while also addressing the challenges of implementing these mechanisms on devices with limited resources.

In conclusion, the discovery of vulnerabilities in BMCs by Nozomi Networks highlights the urgent need for a comprehensive and multifaceted approach to securing in-

dustrial control systems and the Internet of Industrial Things. Failure to address these vulnerabilities can have devastating consequences, not only for the financial well-being of organizations but also for human lives.

Acknowledgment

This study was developed in the context of the Master of Cybersecurity Programme at the Polytechnic University of Viana do Castelo, Portugal.

This work was supported by the Norte Portugal Regional Operational Program (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF), within the project "Cybers SeC IP" (NORTE-01-0145-FEDER-000044).

References

1. Nozomi Networks Labs. Vulnerabilities in BMC Firmware Affect OT/IoT Device Security – Part 1, nov 2022.
2. Lanner Electronics Inc. IAC-AST2500 — Network Appliance — uCPE SD-WAN— MEC Server — Intelligent Edge Appliance.
3. AMI. Megarac.
4. American Megatrends. System-on-Chip Remote Management Toolset MegaRAC SP-X. (Accessed on 20/12/2022).
5. Jalindar Karande and Sarang Joshi. Real-Time Detection of Cyber Attacks on the IoT Devices. In *Real-Time Detection of Cyber Attacks on the IoT Devices*, 2020.
6. Christos Xenofontos, Graduate Student Member, Ioannis Zografopoulos, Charalambos Konstantinou, Senior Member, Alireza Jolfaei, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies; Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies. *IEEE Internet of Things Journal*, 9(1), 2022.
7. Tobias Latzo, Julian Brost, and Felix Freiling. BMCLeech: Introducing Stealthy Memory Forensics to BMC. *Forensic Science International: Digital Investigation*, 32, apr 2020.
8. Jessie Frazelle. Opening up the baseboard management controller. *Communications of the ACM*, 63(2):38–40, jan 2020.
9. Jessie Frazelle. Securing the Boot Process. *Queue*, 17(6):5–21, dec 2019.
10. Dan Farmer. Sold Down the River. (Accessed on 20/12/2022), jun 2014.
11. National Institute of Standards and Technology. CWE - CWE-787: Out-of-bounds Write (4.9).
12. Yoni Shohet. Ransomware Attacks Hit Manufacturing - Are You Vulnerable?, mar 2019.
13. Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and Katherine Banks. A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, 146(5), jan 2020.
14. Martin Giles. Triton is the world's most murderous malware, and it's spreading, mar 2019.
15. Salim Mahamat Charfadine, Olivier Flauzac, Florent Nolot, Cyril Rabat, and Carlos Gonzalez. Secure exchanges activity in function of event detection with the sdn. In Gervais Mendy, Samuel Ouya, Ibra Dioum, and Ousmane Thiaré, editors, *e-Infrastructure and e-Services for Developing Countries*, pages 315–324, Cham, 2019. Springer International Publishing.
16. Jaedeok Lim, Seongyoung Sohn, and Jeongnyeo Kim. Proposal of smart segmentation framework for preventing threats from spreading in iot. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1745–1747, 2020. (Accessed on 23/12/2022).
17. Jane Wakefield. Huge fines and a ban on default passwords in new UK law, nov 2021.
18. Charalambos Konstantinou. Derauth: A battery-based authentication scheme for distributed energy resources. In *Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI*, pages 560–567. IEEE Computer Societyhelp@computer.org, July 2020. Generated from Scopus record by KAUST IRTS on 2022-09-13.

19. Ioannis Zografopoulos, Juan Ospina, and Charalambos Konstantinou. Special session: Harness the power of ders for secure communications in electric energy systems. In *2020 IEEE 38th International Conference on Computer Design (ICCD)*, pages 49–52, 2020.

Shoulder Rehabilitation: Gamified Approach with Data Collection

Moisés Moreira[1], Duarte Duque[1], and Vitor Carvalho[1]

2Ai, School of Technology, IPCA, Portugal
mmoreira@ipca.pt, dduque@ipca.pt, vcarvalho@ipca.pt

Abstract. The use of Head-Mounted Display Virtual Reality (HMD-VR) in physiotherapy is now vastly spread. This emerging approach shows promise in upper limb rehabilitation being our focus on shoulder rehabilitation. However, a significant issue is described in all sort of physiotherapy rehabilitation from low adherence to exercise programs. Current tools for monitoring exercise frequency and correctness are insufficient and with limited focus on data recording. In the other part of the spectrum there are the HDM-VR games that help keeping the patient motivated and showed to be efficient but won´t monitoring the patient during the exercise.
To address these issues this study propose an HDM-VR game for physiotherapy with data collection in immersive environment enhanced with visual cues, color, and haptic feedback, that aims to enhance the rehabilitation experience by promoting proper posture and adherence to exercise metrics. Furthermore, several studies proved that the Oculus Quest 2 is a reliable tool to gather data about the exercises. So, by collecting data during gaming sessions, this will be monitoring the patients' progress, provide valuable insights for both patients and medical professionals and dynamically adapt the game based on individual progress of the patient.

Keywords: HMD-VR · Serious Games · Shoulder Rehabilitation · Data Record

1 Introduction

1.1 Growing Use of VR in Physiotherapy

With the growing body of literature connecting the utilization of HMD-VR (Head-Mounted Display Virtual Reality) and physiotherapy, recent research and trials have contributed substantially to the advancement of this field. Remarkably, [1] Naqvi et al. and [2] Phelan et al. both express favorable remarks concerning the implementation of the HMD-VR approach in the upper limb (UL) rehabilitation.

1.2 Problem: Low Adherence in Patients Exercise Programs

In this field there is a problem with exercise adherence by the patients, as stated by [3]Holden, unsupervised home exercise programs tend to have a adherence less than 50%, more recently.
Furthermore [4] David Burns et al. recognise the same problem they reference that "It is unknown how often patients perform their home exercises and if these exercises are performed correctly". At the time, they also added "there are no established tools for measuring this".

1.3 Solution: Utilizing Effective VR Games for Physiotherapy and Data Collection

In their Longitudinal Cohort Study [4], David Burns et al. put forth the proposal of utilizing a Smart Watch as a monitoring device. However, considering the potential in

HMD-VR, the device could do the monitoring and data record proposed and considering the potential of HMD-VR, this can explore beyond monitoring and data collection. By utilizing HMD-VR, there is the opportunity to create a virtual environment that enhances the rehabilitation experience using one device for all these applications.

1.4 Validity and Precision of the Data Gathered

Studies by [5] Carnevale et al. have demonstrated the accuracy of the Oculus Quest 2 in gathering meaningful data, specially for shoulder rehabilitation. By applying their findings, the approach propose here that will also include measurement and comparison against other certified measuring systems to ensure comparable accuracy.
While further studies are necessary to explore the applicability of this technology in other areas, our assessment will contribute for this growing body of literature, specifically for shoulder rehabilitation by applying this findings in our project and expand it with tests of our own.

2 The Game Phase

2.1 Game Driven Physiotherapy

This study is aimed to support a serious game, where it will integrate a series of exercises in one video game - a definition for serious games can be found [6] in the book Clinical Simulation, Bruno Bonnechère "Serious games are a set of solutions developed to make a whole series of rehabilitation sessions more fun and less boring. A generally accepted definition is 'video games developed for a primary purpose other than pure entertainment' ".
There is no doubt that commercial games are being used to experiment in this field as can be accessed in the studies referenced as [1, 7–9] - they have different degrees of success in rehabilitation - a systematic review would be needed to access if custom made games are more efficient - but this point stands that they are more flexible and in the study here proposed, they allow a seamless integration of the exercises and data collection. Reading [7] Gustavsoon in the section about personalising, in a custom made game all of these variables are flexible and it is easy to preserve the medical validity of the exercise.

2.2 Resources

The game uses the Unity game engine, with the Oculus SDK for Unity to facilitate the integration and data record. The data is stored in a SQL server and all communications follow a RESTful API architectural style. Our hardware is the Oculus Quest 2 with controllers.

2.3 Integration of a Exercise

In the initial approach, the integration of the [10] Passive External Rotation exercise from the Rotator Cuff and Shoulder Conditioning Program was implemented. The

game concept is to cut a trunk with a saw. As illustrated in the next figure 1, the game give feedback using colors, tool-tips and haptic feedback. Additionally, there is an underlying system that operates outside the visible game interface. This system manages the exercise and collects raw data from the HMD-VR set and controllers. For example, in the game, the hands are represented by the color green when they are in the correct position. However, if the patients deviate from the correct posture, the hands turn red. Simultaneously, the controllers vibrate to provide feedback, and as the patients correct their posture, the vibration intensity decreases until it ceases completely, and the hands regain the green color.

Fig. 1: The left half of the image showcases the immersive game environment as a view of the player. On the right side there are options displayed for haptic feedback and measurements - this is not visible to the player.

3 System Description

3.1 The Collected Data

At the time of writing, the accuracy of the Oculus Quest 2 remains a topic of discussion. However, a dedicated study by [5] Carnevale et al. focused on assessing its precision in shoulder rehabilitation . The study concluded that the Oculus Quest 2 exhibits rotational and translational tracking accuracy, providing strong indications of its precision. Based on these findings, this study will record that information during the exercises.
Recognizing the recent advancements in this field, we emphasize the importance of capturing comprehensive data by leveraging the capabilities of the Oculus Quest. In addition to exercise-specific information, we meticulously collect data pertaining to rotation, position, and time stamps during each collection. By incorporating these variables, our goal is to develop a more nuanced understanding of the correlations and relationships present within the data.
All of the gathered data is saved and associated with each patient. In addition to the collected data, supplementary patient information such as age, medical conditions and

the number of sessions attended was also record. This comprehensive approach enables us to expand upon and establish connections between the collected data and the specific characteristics relating patients, therapy and condition.

3.2 System's Architecture

Our system architecture is built upon the capabilities of Unity, as it serves as the foundation for gathering the data obtained from the Oculus Quest.
Once the data is collected, our system seamlessly transfers it to the Cloud for further storing and processing. Within the Cloud, an API acts as a mediator, enabling efficient communication between the game, the Cloud infrastructure and any other system that needs the data (Figure 2). The API will send processed data if needed, once identified the needs of each service and apps that will use the API, will be clear which data should be send. Although, the raw data will always be preserved.
Our system software took concepts from [11] Carlos Nave et al. Mainly will also store

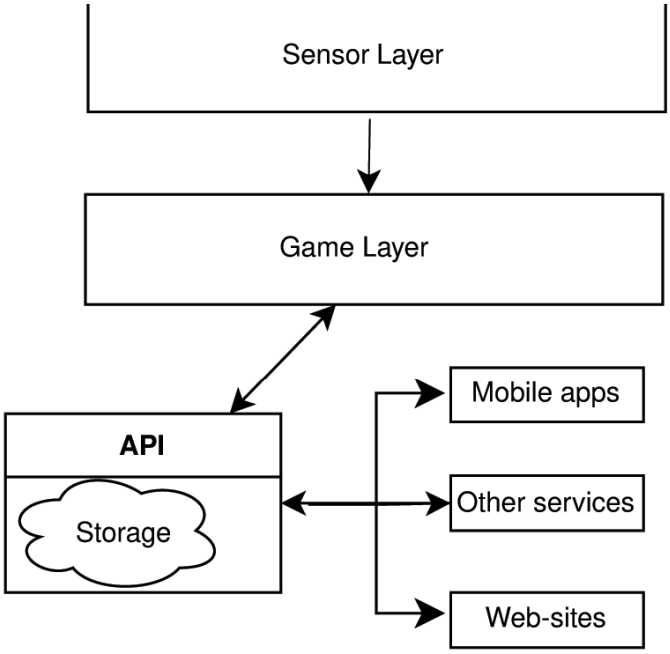


Fig. 2: System's architecture.

our data in a MySQL, even thought, comparing with [11] Carlos Nave et al. diagram for the data collection, we also have the concept of a Patient, Session, Exercises, but the main difference would be that our Session, is not just the data collected but also have the exercises itself in there relationship - our database diagram needs more iterations until can be presented as a solid foundation for this kind of data collection.

A major difference is in the software technologies we use, our server is a Node.js server that uses Express framework that manages a Restfull API, instead of PHP, as it was demonstrated in there article [12] comparing PHP, Python, and Node.js, Kai Lei et al, show that Node.js is better for supporting larger systems than the other two alternatives.

4 Final Remarks

Our study aim to utilize the collected information not only in applications and websites designed to track patients' progress and assist physicians in making informed decisions but also to leverage this expanding dataset for validating the accuracy of equipment and enhancing the design of physiotherapy games. As this project is currently assessing the feasibility and use cases of the system, the specific designs have not been fully developed yet.
Our initial system's architecture resembled the one presented by [11] Carlos Nave et al, but since the devices are different that reflects in our system specifications and as the software and hardware technologies improve the choices and possibilities, for a comprehensive, holistic and integrated system for physiotherapy rehabilitation.

References

1. Naqvi, W.M., Qureshi, M.I., Nimbulkar, G., Umate, L.: Gamification for distal radius fracture rehabilitation: A randomized controlled pilot study. Cureus (9 2022). https://doi.org/10.7759/cureus.29333
2. Phelan, I., Furness, P.J., Dunn, H.D., Carrion-Plaza, A., Matsangidou, M., DImitri, P., Lindley, S.: Immersive virtual reality in children with upper limb injuries: Findings from a feasibility study. Journal of Pediatric Rehabilitation Medicine **14**, 401–414 (2021). https://doi.org/10.3233/PRM-190635
3. Holden, M.A., Haywood, K.L., Potia, T.A., Gee, M., McLean, S.: Recommendations for exercise adherence measures in musculoskeletal settings: A systematic review and consensus meeting (protocol). Systematic Reviews **3** (2 2014). https://doi.org/10.1186/2046-4053-3-10
4. Burns, D., Razmjou, H., Shaw, J., Richards, R., McLachlin, S., Hardisty, M., Henry, P., Whyne, C.: Adherence tracking with smart watches for shoulder physiotherapy in rotator cuff pathology: Protocol for a longitudinal cohort study. JMIR Research Protocols **9**, e17841 (7 2020). https://doi.org/10.2196/17841
5. Carnevale, A., Mannocchi, I., Sassi, M.S.H., Carli, M., Luca, G.D.D., Longo, U.G., Denaro, V., Schena, E.: Virtual reality for shoulder rehabilitation: Accuracy evaluation of oculus quest 2. Sensors **22**, 5511 (7 2022). https://doi.org/10.3390/s22155511
6. Pilote, B., Chiniara, G.: Chapter 2 - the many faces of simulation. In: Chiniara, G. (ed.) Clinical Simulation (Second Edition), pp. 17–32. Academic Press, second edition edn. (2019). https://doi.org/https://doi.org/10.1016/B978-0-12-815657-5.00002-4, https://www.sciencedirect.com/science/article/pii/B9780128156575000024
7. Gustavsson, M., Kjörk, E.K., Erhardsson, M., Murphy, M.A., Kj€, E.K.: Virtual reality gaming in rehabilitation after stroke-user experiences and perceptions (2021). https://doi.org/10.1080/09638288.2021.1972351, https://www.tandfonline.com/action/journalInformation?journalCode=idre20
8. Tran, J.E., Fowler, C.A., Delikat, J., Kaplan, H., Merzier, M.M., Schlesinger, M.R., Litzenberger, S., Marszalek, J.M., Scott, S., Winkler, S.L.: Immersive virtual reality to improve outcomes in veterans with stroke: Protocol for a single-arm pilot study. JMIR Research Protocols **10** (5 2021). https://doi.org/10.2196/26133
9. Tuck, N., Pollard, C., Good, C., Williams, C., Lewis, G., Hames, M., Aamir, T., Bean, D.: Active virtual reality for chronic primary pain: Mixed methods randomized pilot study. JMIR Formative Research **6** (7 2022). https://doi.org/10.2196/38366
10. Rotator cuff and shoulder conditioning program stretching exercises 1. pendulum

11. Nave, C., Postolache, O.: Smart walker based iot physical rehabilitation system. 2018 International Symposium in Sensing and Instrumentation in IoT Era, ISSI 2018 (11 2018). https://doi.org/10.1109/ISSI.2018.8538210
12. Lei, K., Ma, Y., Tan, Z.: Performance comparison and evaluation of web development technologies in php, python, and node.js. In: 2014 IEEE 17th International Conference on Computational Science and Engineering. pp. 661–668 (2014). https://doi.org/10.1109/CSE.2014.142

Artificial Intelligence to Identify Olive-Tree Diseases

Rui Silva[1], João Mendes[2], José Lima[2,3], and Ana I. Pereira[2,3]

[1] Instituto Politécnico de Bragança,5300-253 Bragança, Portugal
a40247@alunos.ipb.pt
[2] Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança,5300-253 Bragança, Portugal
{joao.cmendes, jllima, apereira}@ipb.pt
[3] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

Abstract. In this study, we aim to develop a convolutional neural network (CNN) based system for identifying the health status of olive tree leaves, including two common diseases, peacock spot and aculus olearius. Although the work is still in its early stages, its objective is well-defined, the starting point is a dataset regarding the health of the olive tree leaves, a dataset that will be pre-processed and used as a basis for training and testing the CNN's models. Our goal is to apply various CNN architectures and techniques, such as transfer learning, data augmentation, and fine-tuning, to optimize the accuracy and performance of the model. This study can potentially contribute to developing an efficient and accurate method for identifying olive tree leaf diseases, which can have practical applications in the agricultural industry and benefit the environment.

Keywords: Convolutional neural networks (CNN) · Olive tree leaves · Peacock spot · Aculus olearius.

1 Introduction

Olive trees have significant global economic, cultural, and environmental importance, especially in the Mediterranean region [1]. The olive tree (Olea europaea L.) is one of the most extensively cultivated fruit trees, with over 11 million hectares [2] of land dedicated to olive cultivation worldwide. Besides being a primary source of olive oil, olives, and other related products, olive trees are also valuable for the prevention of soil erosion [3] and desertification [4] if well treated and managed, carbon sequestration [1], and biodiversity conservation [5].

In Portugal, olive cultivation has a long history and represents an important part of the country's agricultural sector. Portugal is one of the major olive oil producing countries in Europe, with 380.412 [6] hectares of olive orchards in 2021 and an annual estimate in 2022 of 126 tons of olive oil [7].

However, olive trees are susceptible to various diseases, pests, and abiotic stresses that can reduce their yield, quality, and longevity. The early detection and diagnosis of olive tree diseases is critical for the sustainable production of high-quality olive products. This can be challenging for farmers who lack experience or knowledge about the tree. Therefore, there is a need to develop accessible and efficient methods for identifying olive tree diseases that can assist farmers in making informed decisions about the management of their olive groves.

In recent years, artificial intelligence techniques, such as convolutional neural networks (CNN's), have shown promise in identifying olive tree diseases based on leaf images [1] [8]. This study aims to develop a CNN-based system for identifying the health

status of olive tree leaves, with a focus on two common diseases in Portugal, peacock spot and aculus olearius. The system is intended as mentioned above for farmers who may not have experience or knowledge about the tree and need a straightforward and practical method to assess the health status of their orchards. By developing an efficient and accessible method for identifying olive tree diseases, this study has the potential to benefit the agricultural industry in Portugal and contribute to decrease the olive production affected by the disease.

This paper is organized as follows. It starts with an introduction, followed by a review of related work. The third section presents the work methodology, including the system architecture and model layout. Finally, the paper concludes summarizing the main findings and suggesting future research directions.

2 Related Work

Identifying diseases in different olive tree species has long been a concern for farmers and researchers. This is a field that, like the others, has undergone several advances in recent times with the application of emerging technologies such as the internet of things, cloud processing, and artificial intelligence algorithms.

In [8] a deep convolutional neural network (DCNN) was suggested to classify aculus olearius illnesses and olive peacock spots. A total of 3400 samples of olive leaves were selected, including healthy leaves, leaves damaged by Aculus Olearius, and leaves with olive peacock spots. Transfer learning techniques were employed on the VGG16 and VGG19 architectures to complete the experimental investigation. A web-based application for this study was also created. The results demonstrated that olive peacock spot and Aculus Olearius could be identified with low mistake rates even without an expert.

Also in [9] focused on experimental work with an agricultural UAV (Unmanned Aerial Vehicle) that flew autonomously over olive groves. Olive leaf diseases would be automatically found and categorized by the UAV. Once the acquired photos were sent there, deep learning algorithms utilized the cloud to identify the precise illnesses affecting olive leaves. A hybrid DL model called MobiRes-Net was suggested to improve the detection of olive leaf diseases. The proposed model achieved an impressive classification accuracy of 97.08%, surpassing the accuracies of the ResNet50 (92.86%) and MobileNet (94.63%) models. It is important to remember that there were certain restrictions on the MobiRes-Net model. First off, because of the underlying modules' complicated structure, it needed longer training and testing runtimes than other models. Furthermore, efficient processing of the models required high-performance hardware.

As it was well established, some works already exist to identify diseases in olive trees using convolutional neural networks. However, all the works cited use pre-trained networks with millions of trainable parameters, making them heavy in terms of processing and size if we think of in loco uses. In this way, one of the objectives of the present work involves the creation of a smaller network that can approach the results achieved in those works, however, with fewer trainable parameters and less need for processing capacity.

3 Methodology

This work aims to develop an artificial intelligence system to identify the two diseases mentioned in our introduction. For that, there is a set of steps to be taken and implemented, thus ensuring the correct and optimal functioning of the system we are trying to create, as depicted in the figure 1.

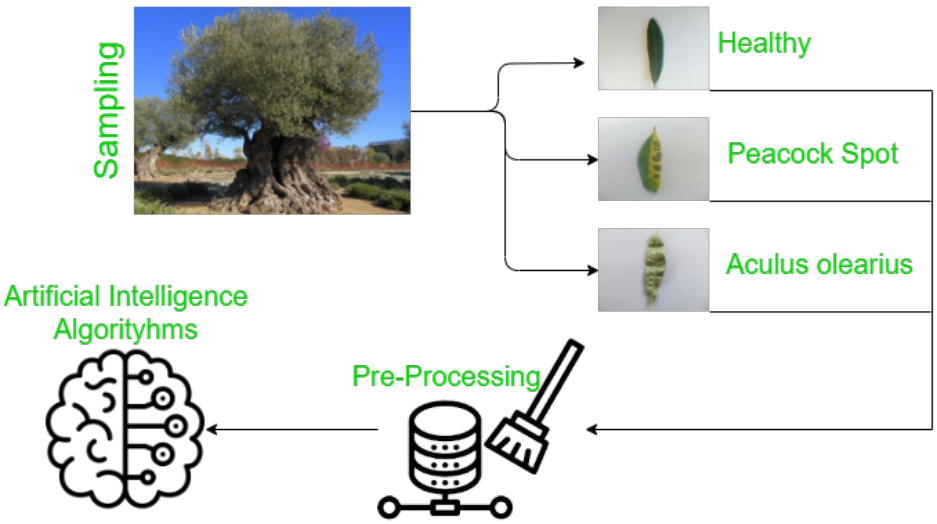


Fig. 1: System architecture.

As a need common to all artificial intelligence problems, the dataset is undoubtedly one of the pillars for the good behaviour of the system. This, despite the simplicity of its creation, is a time-consuming process, as it is necessary to guarantee a large amount of leafs and the entire process of storing and photographing them. Contributing to the difficulty of this process and considering the problem in question, it is important to emphasize that not all trees show disease symptoms, making it even more difficult to collect material to train the algorithms. This way, an extensive search was carried out on the web, trying to find datasets that fit our problem. During this research, a dataset from Turkey was found with 3400 examples of three different categories (healthy, peacock eye, and Aculus Olearius), which was the same dataset used in the first related work written above. It was decided to use the dataset in question to validate these diseases with the incidence rates in the region and the similar climate between the collection point and our region.

Despite being a very homogeneous dataset, several processes were carried out to guarantee the correct functioning of the artificial intelligence algorithms. Pre-processing starts with homogenizing the size of the images, resizing them all to a size of 299x299x3 using RGB (Red, Green, Blue) images. The second step of the pre-processing consisted of the evaluation of repeated items, this is an essential process when working with unknown datasets since we may be causing an unnecessary bias in the artificial intelli-

gence algorithms if this point is not validated. To this end, and taking into account the dimensions of the dataset, autonomous methods were used, comparing the operation of three methods for this purpose, whichever method gives more satisfactory results will be used in our system.

After completing the explanation regarding the methodology, the artificial intelligence model that will be studied will now be presented. Analysing the related works, this work aimed to explore an aspect other than transfer learning. In this way, the model presented here results from a ground-up implementation that will bring advantages in terms of the model's speed and the necessary processing capacity, reducing the number of parameters compared to other models such as the traditional VGG's networks. However, if we discover that it not best suits our needs, we may still change its layers and parameters. Talking about the layers, the figure 2 below represents our model layout.

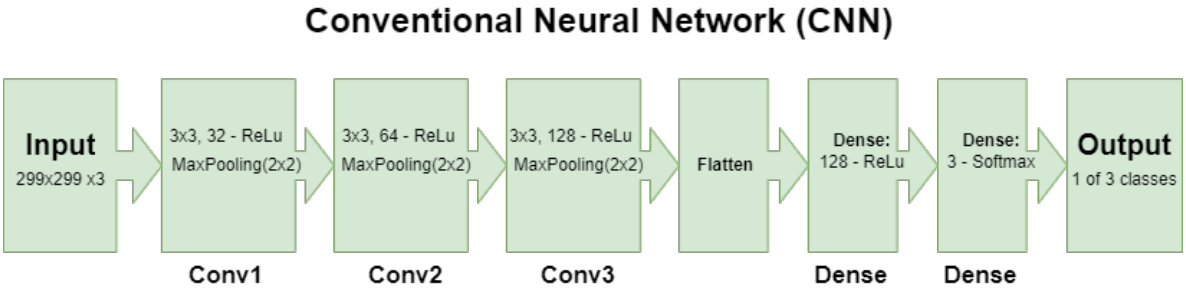


Fig. 2: Model layout.

Our model has a total of 5 layers. The input receives the images we want to classify, these images have a specific size (299x299) and three-colour channels (red, green, and blue).

We have a series of convolutional layers that extract features from the images. These layers apply filters to the images to detect important patterns, such as edges, shapes, and textures. Each layer has a certain number of filters (e.g., 32, 64, 128) that are learned during training to find the best representation of the data.

After each 'Conv2D' layer, there is a 'MaxPooling2D' layer. This layer decreases the size of the feature maps, while preserving the most important features.

Following the convolution and max pooling layers, we have a 'Flatten' layer that transforms the data into a one-dimensional vector. This is necessary to connect this feature extraction part to the dense layers.

The dense layers are like additional neurons that receive the extracted features and perform mathematical operations to classify the images into categories. The first dense layer has 128 neurons and uses an activation function called 'ReLU'. The second dense layer, which is the last layer of the model, represents the output layer. It consists of several neurons equal to the number of classes to be classified (e.g., 3 categories). The activation function used in this layer is 'Softmax', which ensures that the output values represent probabilities, indicating the likelihood of belonging to each class. The

softmax function normalizes the outputs, sums them up to 1 and provides a measure of confidence or certainty in the classification.

4 Conclusion and future work

As it was possible to prove with the cited papers in Section 2 some works already propose similar approaches in different cultures, demonstrating the possibility of the success of the presented study.

The study's primary ongoing tasks will be to complete the comparison of the three pre-processing techniques, after this comparation the best one will be chosen to use in the final model. Apart to this, other techniques will be used to improve the generalization of the model, techniques like data augmentation, some examples could be the vertical and horizontal shift, also vertical/horizontal flip, rotation, brightness adjustment in order to understand what impact those can have on the accuracy of the models.The ultimate goal is to include the most prevalent diseases in Portugal in the system to create an all-encompassing system. Other ideas we could explore include creating a user interface via an intuitive application that aims to make it possible for the user to determine whether their olive orchards are healthy or suffer from the specified diseases above.

References

1. A. Galán-Martín, M. M. Contreras, I. Romero, E. Ruiz, S. Bueno-Rodríguez, D. Eliche-Quesada, and E. Castro-Galiano. The potential role of olive groves to deliver carbon dioxide removal in a carbon-neutral europe: Opportunities and challenges. *Renewable and Sustainable Energy Reviews*, 165:112609, 2022.
2. P. DeAndreis. 5.5 million hectares of traditional olive groves at risk of abandonment.
3. C. Kosmas. Land use: Olives.
4. International Olive Council. The world's olive forest protects against co2.
5. Infrastructure European Climate and Environment Executive Agency. "olives for life" connect agriculture and biodiversity.
6. Pordata. Superfície das principais árvores de fruto e oliveiras.
7. M. M. Tiago. Produção de azeite caiu 40%, mas campanha de 2022 será a quarta maior de sempre.
8. S. Uğuz and N. Uysal. Classification of olive leaf diseases using deep convolutional neural networks. *Neural Computing and Applications*, 33, 05 2021.
9. A. Ksibi, M. Ayadi, B. Soufiene, M. M. Jamjoom, and Z. Ullah. Mobires-net: A hybrid deep learning model for detecting and classifying olive leaf diseases. *Applied Sciences*, 12(20), 2022.

An Analysis of Threats on Top-Level Domains Using File Type Extensions

Anderson Sales[1], Nuno Torres[1], and Pedro Pinto[1,2]

[1] ADiT-Lab, Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal
ansales@ipvc.pt, nunotorres@ipvc.pt, pedropinto@estg.ipvc.pt
[2] INESC TEC, 4200-465 Porto and Universidade da Maia, 4475-690 Maia, Portugal

Abstract. With the increasing number of Top Level Domains (TLDs) being introduced, the potential for security risks and vulnerabilities also increases. A particular concern arises when ambiguity is created between TLDs and file extensions, leading to potential confusion and security threats. This article addresses the risks associated with TLDs that utilize identical file extensions. The overlapping use of TLDs and file extensions creates potential security loopholes and exposes users to significant risks, as attackers may exploit this ambiguity to compromise user security. By enumerating and exemplifying different vulnerability scenarios resulting from the overlap between TLDs and file extensions, it is possible to provide a comprehensive landscape in understanding the potential threats arising from this ambiguity. This paper underlines the significance of understanding and addressing the risks associated with TLDs that share identical file extensions. Additionally, it analyzes the potential vulnerabilities of TLDs with identical file extensions, illustrating how attackers can exploit them to compromise user security.

Keywords: Top-level domain · file extensions · security threats · cyber security · cyber attack

1 Introduction

Top Level Domains are fundamental elements of the Internet's domain name structure. They are located at the top of the domain name hierarchy and provide a logical categorization of web addresses. Each TLD has a specific set of rules and restrictions defined by the organization responsible for administering it. Furthermore, they play a crucial role in identifying and differentiating websites by providing information about the nature and origin of online resources.

The TLDs specification is part of the operation of the Domain Name Services (DNSs). Their fundamentals and use of Uniform Resource Locators (URLs) are defined in [1], which outlines general guidelines for the structure and delegation of domain names, including TLDs. Additionally, in [2] and [3] the support for domain names is specified, including the hierarchical structure of TLDs. The most common TLDs can be listed as follows:

1. Generic top-level domains (gTLD)
2. Sponsored top-level domains (sTLD)
3. Country code top-level domains (ccTLD)

These types distinguish IANA [4] related domains and Country code top-level domains (ccTLDs). For instance, ".co.uk" and ".pt", are used to represent specific countries or regions, while ".com", ".org", and ".net" are classified as generic top-level domains (gTLDs) along with ".zip". Additionally, ".gov", ".edu", and ".mil" are sponsored top-level domains (sTLDs).

Understanding these concepts is crucial for navigating the web securely. A typical URL consists of several parts, each serving a specific purpose, including the scheme or protocol, a domain name with TLDs, path, and additional parameters. Familiarity with these URL elements empowers users to identify and assess potential security risks associated with TLDs and file extensions.

By recognizing and verifying the different parts of a URL, users can make the right decisions when interacting with online content, mitigating the risk of falling prey to malicious websites or files disguised as legitimate resources. Therefore, a more comprehensive understanding of how TLDs fit into the broader URL structure enhances users' abilities to navigate the web safely and protect themselves from cyber threats. Figure 1 explains the parts of a URL.

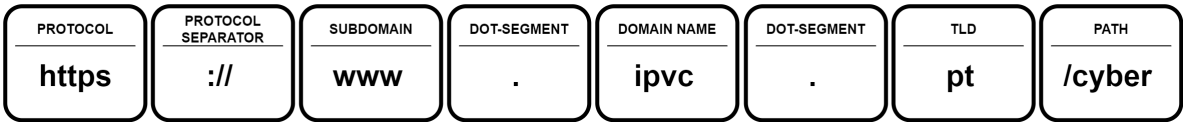


Fig. 1: Example of a URL structure.

In turn, file extensions are suffixes added to file names to indicate their type or format. They provide important information about how a file should be interpreted and processed by the operating system or application. For example, the extensions ".docx" and ".pdf" indicate Microsoft Word document files and Portable Document Format (PDF) files, respectively. By correctly identifying file extensions, systems can apply appropriate actions, such as opening the file with the appropriate application or taking security measures.

The ambiguity between file extensions and TLDs became apparent when Microsoft launched DOS in 1981, using file extensions with the ".com" extension. However, this coincidence did not represent a cybersecurity disaster, as the two are independent and can be easily distinguished.

Nowadays, cyber security has become a critical concern as cyber threats are constantly evolving. Targeted attacks, phishing, malware distribution, and exploiting vulnerabilities are just a few examples of threats that can compromise the integrity, confidentiality, and availability of systems and data.

To mitigate these threats, it is crucial to recognize the potential risks associated with TLDs that share identical file extensions and proactively address this concern.

This article is organized as follows. Section 2 presents the related work. Section 3 explores different threat scenarios related to web security and file manipulation. Section 4 provides the discussion regarding the main vulnerabilities and threat scenarios. Section 5 addresses the conclusions and future research.

2 Related Work

The DNSs service can be the target of a variety of attacks, including DNSs cache poisoning attacks according to the study presented by the authors in [5]. In this type

of attack, an attacker manipulates the cache records of the DNSs server with false and malicious information. When legitimate users send requests to the DNSs server, they receive false responses, leading them to be redirected to malicious websites or compromising their information.

Furthermore, DNSs can also be exploited in other scenarios, such as DNSs amplification for Distributed Denial of Service (DDoS) attacks as stated in article [6], where an attacker manipulates the DNSs server to send large responses to the IP address of a target, causing disruptions by overloading it with traffic. This concern about the security and stability of DNSs has driven an increase in studies related to the use or abuse of TLDs operators. As a result, researchers have focused on measures to enhance DNSs security and stability, including addressing TLDs operators in a broader context.

A number of research works are focused on the use or misuse of TLDs operators. In [7], the authors addressed DNSs security and stability through a control plane for TLDs operators. While its focus is on DNSs security in general, the considerations addressed in this research may offer insights into mitigating vulnerabilities in specific TLDs, including cases where identical file extensions may pose security risks.

The authors in [8] analyzed DNSs configurations and their security by examining resource records of TLDs. Although not exclusively focused on TLDs with identical file extensions, the analysis of DNSs configurations can provide valuable information on how to avoid ambiguities and associated security risks.

The article [9] presented research on detecting malicious domains using statistical Internationalized Domain Name features in TLDs. While this work focuses on detecting malicious domains, it can offer insights into identifying potential TLDs with identical file extensions that attackers may exploit.

The work [10] explored the evolution and adoption of TLDs and DNSSEC. Although its focus is broader, understanding the evolution of TLDs can help contextualize the issue of identical file extensions and their implications for cybersecurity.

Based on recent reports and research, the potential risks associated with the use of common file extensions as TLDs have become a growing concern. Trend Micro's research [11] highlights the emergence of using file extensions as TLDs, presenting a possible future exploitation vector; where such ambiguity can result in security loopholes, as also reported by [12]. Additionally, Kaspersky [13] also underscores the significant concern that this new scenario will bring to the cyber world, further reinforcing the need to understand this new landscape and adopt countermeasures for protection.

Considering these related works, this article contributes to strengthening the knowledge of the threats and vulnerabilities associated with TLDs with identical file extensions. These research contributions enhance the broader understanding of the Internet security landscape and aid in identifying effective solutions to mitigate the risks posed by this overlap between TLDs and file extensions.

3 Vulnerability and Threat Scenarios

This section explores a set of vulnerabilities and threat scenarios, arising from the ambiguity between TLDs and file extensions. The overlap between these two elements can create security loopholes and expose systems and users to significant risks.

Figure 2 shows a few examples of TLDs and file extensions that can be used to create Internet domains.

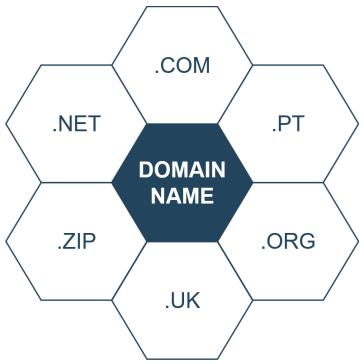


Fig. 2: Example of TLDs.

Understanding attack scenarios is crucial for developing effective protection strategies. Thus, they can depicted as follows:

1. Open Redirect attacks - it is possible to combine the Open Redirect attack with trusted TLDs to a malicious URL with ".zip" extensions and deceive users. For instance, the legitimate website:
   https://go.dev/dl/linux-amd64.zip
   may have an open redirect pointing to a malicious website like:
   https://go.dev/dl/@linux-amd64.zip
   when checking the Uniform Resource Identifier (URI) parsing any element before the "@" will be ignored by the browser and will forward the end user to the malicious domain linux-amd64.zip.
2. Phishing - In this scenario, phishing scams make use of the ".zip" TLDs to host websites that resemble legitimate download portals. Unsuspecting users can be tricked into believing that they are downloading an authentic ".zip" file when, in reality, they are being redirected to a malicious website. Using the ".zip" TLDs helps mask malicious links as legitimate file downloads, thereby increasing the effectiveness of phishing attacks and the success rate of deceiving victims. A more detailed view of the phishing attack is shown in Figure 3.
3. Malware Delivery - In the context of TLDs and file extensions, malware delivery involves the use of deceptive elements to direct users to malicious websites, where malware is delivered and implanted on users' systems. In this scenario, attackers exploit the ambiguity between TLDs and file extensions to create fake URLs that redirect users to fraudulent websites. By visiting these sites, users may be tricked into downloading or executing malicious files, resulting in their systems being infected.
4. Supply Chain Attack - Threat actors can compromise the supply chain of legitimate software, or service, by inserting malicious ".zip" files with misleading TLDs. When downloaded and executed by users, these files can introduce malware into systems

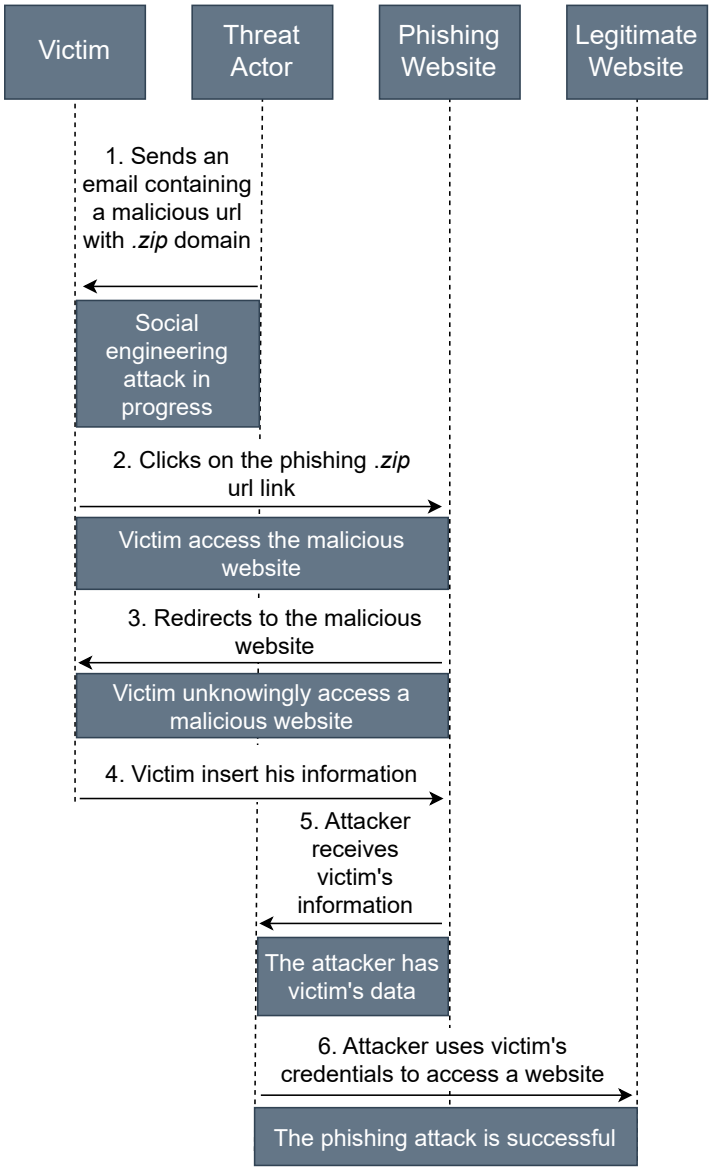


Fig. 3: Example of Phishing.

as they are perceived as legitimate files. A more detailed view of the Supply Chain attack is depicted in Figure 4.

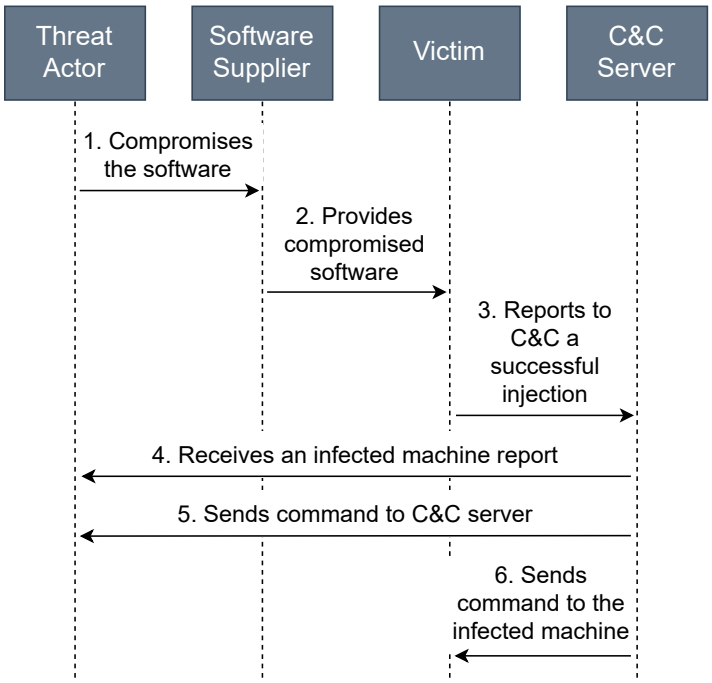


Fig. 4: Example of Supply Chain.

5. Cryptocurrency Mining Scripts - Hackers can host websites with the ".zip" TLDs that automatically run cryptocurrency mining scripts on visitors' machines. These scripts can be disguised as part of the process of downloading or unpacking files. The rationale for downloading a ".zip" file may serve as an explanation for the high CPU consumption, typically associated with cryptocurrency mining, thereby reducing the likelihood that users will suspect and identify malicious activity.
6. Domain Spoofing - In this kind of attack threat, actors can create websites using the ".zip" TLDs, which are designed to closely resemble the legitimate domains of trusted organizations. The aim is to trick users into providing confidential information or performing malicious actions. Using the ".zip" TLDs on these spoofed domains can bring an additional appearance of legitimacy, making it more likely to trick unsuspecting users into trusting and interacting with the malicious website. For instance, a legitimate domain hosting a download file such as
   https://go.dev/dl/go1.20.1.linux-amd64.zip
   can easily be spoofed to the following malicious website:
   https://go.dev.dl.go1.20.1.linux-amd64.zip
7. Shortcut Disguise Attack - This kind of attack involves creating shortcuts or links that appear to be legitimate ".zip" files. These shortcuts are designed to trick users into believing they are opening a ".zip" file, but direct them to a malicious website when clicked. This site may contain different threats such as malware downloads or

phishing pages. The strategy behind this attack is to exploit users' familiarity with ".zip" files and the confidence they have in opening these files. By disguising the shortcut as a ".zip" file, attackers increase the likelihood that users will fall into the trap, thereby compromising their security.

8. Data Exfiltration - Threat actors can utilize ".zip" TLDs as part of their command and control infrastructure, allowing data exfiltration from compromised systems by making it appear as if that data is being uploaded to a harmless ".zip" file. Using the ".zip" TLDs also assists in concealing the whereabouts of stolen data. This tactic aims to bypass protective measures and allow attackers to discreetly obtain confidential information.
9. Drive-By Downloads - Cybercriminals can take advantage of the ".zip" TLDs to perform automated downloads, in which a website downloads a malicious file onto a user's system without their knowledge or consent. Using the ".zip" TLDs can make these malicious downloads appear more legitimate, making them more difficult for users and security software to detect and block. This technique seeks to exploit users' trust when accessing websites that appear to be harmless, resulting in the silent infiltration of malware.
10. Social Media Spambots - Criminals can use websites with the ".zip" TLDs to host malicious content or links, which are then spread through social media spambots. These links may pose as "unique" downloads or "leaked" files to trick users into clicking on them. Using the ".zip" TLDs can make these links appear to be harmless file downloads, which increases click-through rates and the potential spread of malware.

4 Discussion

The findings reported in this paper, shed light on the potential cybersecurity risks associated with TLDs that share identical file extensions. Among the mapped scenarios, it can be highlighted greater concern with phishing and supply chain attacks.

Phishing attacks are well-known for exploiting users' trust and leading them to malicious websites through deceptive URLs. Using TLDs like ".zip" could create opportunities for attackers to design URLs, that mimic authentic file downloads. Attackers can exploit this ambiguity to deceive users, leading them to open suspicious files or visit malicious websites to perform this kind of attack.

Regarding Supply Chain Attacks, threat actors have demonstrated a propensity for exploiting vulnerabilities in software or service updates. This is one of the types of attacks that can have the greatest relevant impact. The SolarWinds case in 2020 [14] exemplifies the severe consequences such attacks can have on organizations and their customers. After this catastrophic cyber incident, it is estimated that the financial loss was approximately $90,000,000, as reported by BitSight [15]. It is essential to remain proactive in identifying and addressing potential weaknesses in the software supply chain, even in cases involving TLDs.

The cybersecurity landscape is ever-evolving, and the identification of potential vulnerabilities helps foster a proactive approach to safeguarding systems and users. This work contributes to the existing literature by bringing attention to the potential risks

and implications of TLDs with identical file extensions, thereby encouraging further research in this area.

5 Conclusion

This work explores threat scenarios related to the ambiguity between TLDs and identical file extensions, which raise concerns in browsing and file manipulation. It aims to identify potential risks and vulnerabilities. It also highlights use cases that are more likely to occur, such as phishing, and those that can cause significant financial impact, such as supply chain attacks.

Some potential areas for future research include evaluating security measures and conducting a sampling analysis of cyberattacks, using open-source intelligence (OSINT) to gain a better understanding of the specific threats associated with this aspect. This can lead to the development of innovative approaches to protect users and their sensitive information.

By addressing these areas, future research can contribute to expanding knowledge and improving security practices on the web, while tackling specific challenges. These investigations can potentially strengthen user protection and enhance the reliability of their online interactions.

References

1. Jon Postel. Domain Name System Structure and Delegation. RFC 1591, Internet Engineering Task Force, 1994.
2. P. Mockapetris. Domain Names - Concepts and Facilities. RFC 1034, Internet Engineering Task Force, 1987.
3. P. Mockapetris. Domain Names - Implementation and Specification. RFC 1035, Internet Engineering Task Force, 1987.
4. IANA. Iana root zone database, 2023.
5. Fatemah Alharbi, Jie Chang, Yuchen Zhou, Feng Qian, Zhiyun Qian, and Nael Abu-Ghazaleh. Collaborative client-side dns cache poisoning attack. In *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pages 1153–1161, 2019.
6. Huiming Yu, Xiangfeng Dai, Tom Baxliey, Xiaohong Yuan, and Terry Bassett. A visualization analysis tool for dns amplification attack. In *3rd International Conference on Biomedical Engineering and Informatics*, volume 7, pages 2834–2838, 2010.
7. Cristian Hesselman, Giovane C.M. Moura, Ricardo De Oliveira Schmidt, and Cees Toet. Increasing dns security and stability through a control plane for top-level domain operators. *IEEE Communications Magazine*, 55(1):197–203, 2017.
8. Mengyuan Wang, Zhaoxin Zhang, and Haiyan Xu. Dns configurations and its security analyzing via resource records of the top-level domains. In *11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, pages 21–25, 2017.
9. Alshaima Almarzooqi, Jawahir Mahmoud, Bayena Alzaabi, Arsiema Ghebremichael, and Monther Aldwairi. Detecting malicious domains using statistical internationalized domain name features in top level domains. *14th Annual Conference on Undergraduate Research on Applied Computing (ZURC2022)*, 2022.
10. Yo-Der Song, Aniket Mahanti, and Soorya Charan Ravichandran. Understanding evolution and adoption of top level domains and dnssec. In *IEEE International Symposium on Measurements & Networking (M&N)*, pages 1–6, 2019.
11. Joshua Aquino and Stephen Hilt. Future exploitation vector file extensions as top level domains, May 2023.
12. Scott Ikeda. New google top-level domains that use common file extensions could pose a serious cyber risk, May 2023.

13. Stan Kaminsky. Security risks of the .zip and .mov domains, May 2023.
14. Jake Williams. What you need to know about the solarwinds supply-chain attack, May 2020.
15. Samit Shah. The financial impact of solarwinds breach, Jan 2021.

Data pruning approach in the retail sector

Felipe G. Silva[1], Inês Sena[1], Laires A. Lima[1], Florbela P. Fernandes[1,2], Maria F. Pacheco[1,2], Clara B. Vaz[1,2], José Lima[1,2], and Ana I. Pereira[1,2]

[1] Research Center in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
{gimenez, ines.sena, laires.lima, fflor, pacheco, clvaz, jllima, apereira}@ipb.pt
[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

Abstract. Workplace accidents remain a significant challenge for companies. Although the application of intelligent systems is a recent development, it has shown promising results in enhancing workplace safety, and there are already highly accurate solutions available for this purpose. However, these solutions only focus on data related to the accident and the victim. Therefore, the aim of this research is to innovate and incorporate various information from a retail company within the sector into future design works for developing an accident forecasting model. To achieve this, it is essential to streamline the datasets by retaining only the essential information. Consequently, this study aims to demonstrate that statistical methods such as the χ^2 test and correlation analysis can reduce the datasets to be used in the future by over 50%.

Keywords: Statistic analysis · Reduction data · Occupational accidents.

1 Introduction

The prevention of accidents at work is a critical issue worldwide. In addition to the financial implications for affected companies, the social impact and loss of human life are the most controversial effects of this important problem [1]. Although companies over the years have implemented prevention actions and improvements in equipment and machinery, these events continue to occur on a high scale, with Portugal in fifth place among the European Union countries with the highest number of accidents at work [2].

Thus, due to advances in Artificial Intelligence, intelligent solutions in the area of occupational safety are beginning to be explored, such as predictive analysis, which has already achieved good precision results for the forecast of accidents at work [3–5], the severity of the events [6–8], the type of accident [9], among other related matters. For that model, the user data is based on the information about the event characteristics of the accident and the rugged employee [10, 11].

However, it is known that companies generate and store a large amount of data over time from different sources, such as internal systems and mobile applications, that can be used as predictors of an accident prediction model. However, it is common knowledge that the good performance of Machine Learning classification/prediction algorithms depends on the data quality. Therefore, it is necessary to include only relevant information.

This study aims to minimize the datasets provided by calculating the relationship between each database's input and output variables. To this end, depending on the

typology of the constituent data, the χ^2 test statistical methods and the Pearson coefficient will be applied to each of the bases individually to find the variables that have a greater impact on the output, achieving the same result with as little information as possible.

The rest of the paper is organized as follows. Section 2 reports the dataset and methods used during preparation. In Section 3 the obtained results are presented. Finally, the study is concluded, and future work is presented in Section 4.

2 Methodology

The retail company provided nine databases for the design of the forecast model for reducing the occurrence of accidents at work in the company:

- **Accidents records** - which contains 145 input variables, with information about the general characteristics of the injured employees (age, seniority, etc.).
- **Accident investigation** - this data set is intended to discover the causes of the accident, being composed of more detailed information such as the reasons why it happened, type of behavior, and the action that originated it, among others, making a total of 57 input variables for the output variable that would be the respective cause of the accident.
- **Near accidents** - contains relevant information about accidents that could have happened and did not happen for some reason. They are divided into 26 input variables.
- **Accidents costs** - is a dataset composed of information regarding the costs involved in the accident, payments for the day of absence, and whether or not it was accepted by the insurer, among others, totaling 30 input variables.
- **Action Plan** - these are plans made after an intervention by third parties or the employees regarding the repair and improvement of working conditions observed during a visit to the store or their working day, respectively. Accounting for 27 input variables.
- **Ergonomic Workplace Assessment (EWA)** - consists of values calculated in the analysis of the postures and movements adopted by an employee in the performance of his duties; these values are given both by the employee in several questions and by technicians through different calculation methods, totaling 106 input variables.
- **Hazard Identification and Risk Assessments (HIRA)** - comprises risk levels associated with each mandatory work task, comprising 31 input variables.

Considering the total number of variables that comprise each database, a total of 422 variables is obtained, a large amount of information that may affect the performance of the classification and/or prediction algorithm that will be used in the future.

It is intended to apply two statistical methods to calculate the relationship between a pair of variables, the χ^2 test and the cooperation analysis using the Pearson coefficient. The χ^2 test was chosen since it establishes the strength of the relationship between two categorical variables, or between categorical and numerical variables, and the Pearson coefficient for cases in which it is intended to calculate the strength of the relationship between two continuous variables. Pearson coefficient was selected from the other coefficients due to the nature of the data following a normal distribution.

The χ^2 test allows us to assess whether there is an independent relationship between the input and output variables, regardless of whether they are numeric or categorical [12]. It is based on observed and expected values. The χ^2 test's null hypothesis (H_0) states that the variables i and j in a contingency table are independent. In contrast, the alternative hypothesis (H_1) states that these variables are not independent. Thus, the null hypothesis is rejected, considering a significance level equal to 0.05, like $p_{value} < 0.05$.

Pearson's coefficient explores whether two normally distributed continuous variables exhibit linear association, assuming values only between -1 and 1, as can be observed in Table 1, which reveals whether they are inversely or directly, respectively [13]. When two variables are inversely proportional, it means that when the value of one variable increases, the other one decreases. On the other hand, when a correlation between variables is directly proportional, it means that when the value of one of the variables increases or decreases the same happens to the other [13].

Table 1: Values of the Pearson coefficient and their characteristics adapted from [14].

Absolute Magnitude of the coefficient	**Interpretation**
0 - 0.30	no correlation
0.31 - 0.50	week correlations
0.51 - 0.70	moderate correlations
0.71 - 0.90	strong correlations
> 0.90	very strong correlations

It should be noted that, except for the EWA base, for calculating the relationship between variables, χ^2 was chosen since they are composed of numerical and categorical variables. Each database contains an output, so we intend to apply both methods individually to each one, relating each input variable with the output one to select the variables that have the greatest impact on the output. In this way, it allows for minimizing the information necessary to obtain the same output. According to Table 1, variables that obtain a positive correlation between 0.50 and 1 are considered for the EWA dataset.

3 Results

Thus, the most appropriate statistical method for the typology of information constituting them was applied for each database, as identified in Table 2.

Analyzing the Table 2 it is observed that initially there were 422 variables and in the end, it accounted for only 220. Using statistical methods, we minimized the information provided by 52.13%

4 Conclusions and Future Works

Through this study, it was revealed that it is possible, through statistical methods, to reduce the information of each database individually greatly (52.13%).

Table 2: Difference between the number of variables before and after application of statistical methods.

Datasets	Initial Variables	Statistical method	Significant Variables
Accidents Records	145	χ^2 Test	45
Accidents Investigation	57	χ^2 Test	19
Near Accidents	26	χ^2 Test	18
Casualty Costs	30	χ^2 Test	21
EWA	106	Pearson Coefficient	82
HIRA	31	χ^2 Test	18
Actions Plan	27	χ^2 Test	17

In the future, it is intended to compare the results obtained, by the various performance evaluation metrics, in the application of several Machine Learning classification algorithms in the different datasets, with and without information reduction, to understand which of the databases obtains better results in terms of performance. This has not yet been possible, as no solution has been found because there is no information about the non-occurrence of accidents.

However, it is expected to apply the reduced databases in the developed prediction model to predict accidents at work in a retail company.

Acknowledgment

The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021). This work has been supported by NORTE-01-0247-FEDER-072598 iSafety: Intelligent system for occupational safety and well-being in the retail sector.

References

1. María Carmen Carnero and Diego Jose Pedregal. Modelling and forecasting occupational accidents of different severity levels in spain. *Reliability Engineering & System Safety*, 95(11):1134–1141, 2010.
2. Pordata. `https://www.pordata.pt/portugal`. Accessed: 2023-04-03.
3. Anuoluwapo Ajayi, Lukumon Oyedele, Olugbenga Akinade, Muhammad Bilal, Hakeem Owolabi, Lukman Akanbi, and Juan Manuel Davila Delgado. Optimised big data analytics for health and safety hazards prediction in power infrastructure operations. *Safety science*, 125:104656, 2020.
4. Fatemeh Davoudi Kakhki, Steven A Freeman, and Gretchen A Mosher. Evaluating machine learning performance in predicting injury severity in agribusiness industries. *Safety science*, 117:257–262, 2019.
5. Fatemeh Davoudi Kakhki, Steven A Freeman, and Gretchen A Mosher. Applied machine learning in agro-manufacturing occupational incidents. *Procedia Manufacturing*, 48:24–30, 2020.
6. Daniel Mesafint Belete and Manjaiah D Huchaiah. Grid search in hyperparameter optimization of machine learning models for prediction of hiv/aids test results. *International Journal of Computers and Applications*, 44(9):875–886, 2022.
7. John D Hunter. Matplotlib: A 2d graphics environment. *Computing in science & engineering*, 9(03):90–95, 2007.
8. Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, et al. Scikit-learn: Machine learning in python. *the Journal of machine Learning research*, 12:2825–2830, 2011.
9. Sobhan Sarkar, Rahul Raj, Sammangi Vinay, J Maiti, and Dilip Kumar Pratihar. An optimization-based decision tree approach for predicting slip-trip-fall accidents at work. *Safety Science*, 118:57–69, 2019.

10. Beatriz Fernández-Muñiz, José Manuel Montes-Peón, and Camilo José Vázquez-Ordás. Relation between occupational safety management and firm performance. *Safety science*, 47(7):980–991, 2009.
11. Charles R Harris, K Jarrod Millman, Stéfan J Van Der Walt, Ralf Gommers, Pauli Virtanen, David Cournapeau, Eric Wieser, Julian Taylor, Sebastian Berg, Nathaniel J Smith, et al. Array programming with numpy. *Nature*, 585(7825):357–362, 2020.
12. Inês Sena, Laires A Lima, Felipe G Silva, Ana Cristina Braga, Paulo Novais, Florbela P Fernandes, Maria F Pacheco, Clara B Vaz, José Lima, and Ana I Pereira. Integrated feature selection and classification algorithm in the prediction of work-related accidents in the retail sector: A comparative study. In *Optimization, Learning Algorithms and Applications: Second International Conference, OL2A 2022, Póvoa de Varzim, Portugal, October 24-25, 2022, Proceedings*, pages 187–201. Springer, 2023.
13. Patrick Schober, Christa Boer, and Lothar A Schwarte. Correlation coefficients: appropriate use and interpretation. *Anesthesia & analgesia*, 126(5):1763–1768, 2018.
14. Hélio Amante Miot. Correlation analysis in clinical and experimental studies, 2018.

Time series forecasting of retail transactions

Rui Melo[1], Inês Sena[1], Felipe G. Silva[1], Florbela P. Fernandes[1,2], Maria F. Pacheco[1,2], Clara Vaz[1,2], José Lima[1,2], and Ana I. Pereira[1,2]

[1] Research Center in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
{ruimelo, ines.sena, gimenez, fflor, pacheco, clvaz, jllima, apereira}@ipb.pt

[2] Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

Abstract. This study uses time series forecasting methods to predict the number of transactions performed for the next 15 days in 8 different sections of a retail company store. Recursive multi-step forecasting was used to solve the problem, and several regression methods were used to determine which would perform better. It was concluded that it is possible to forecast the number of transactions for this case, obtaining a mean absolute percentage error between 0.085 and 0.167 among the 8 sections.

Keywords: Time series · Multi-step forecasting · Regression

1 Introduction

Accidents may occur in the workplace, putting the health and well-being of the employees at risk. Therefore, it is in the interest of all industries to reduce the number of occupational accidents and their severity. As such various practices have been attempted such as enforcing safety protocols [5], applying *LEAN* tools in risk management [11], and even implementing advanced machine learning algorithms to detect whether workers are complying or not with safety regulations [8].

In this work, continuous data on the number of transactions per section of a retail store will forecast how many transactions were made in each section for the next 15 days. With this forecast it will be possible to estimate how many customers visit each section daily, allowing the supervisors to adjust the schedule of the employees thus reducing strain caused by overworking and consequently decreasing the risk of an accident.

The multi-step forecasting method was used with several regression algorithms to achieve this goal. This is a methodology that can be used whenever the data is a time series, and it has been used in the past for various areas such as forecasting tax collection [10], wind speed [12], and traffic speed [14].

This study intends to use a dataset consisting of 572 consecutive days of transaction data to determine which regression algorithm performs better. Based on historical data, the objective is to predict the daily transaction count within 8 sections of a retail store for the upcoming 15 days.

This paper is organized as follows. Section 2 describes in detail the time series data and how they can be used to predict future events through the underlying patterns present in the data and a literature review of existing methods. Section 3 presents the results obtained. Finally, Section 4 summarizes the study's findings and suggests future research directions.

2 Methodology

This section presents the dataset used, the tested regression methods, the error calculation, and the validation methods to achieve the listed objectives.

2.1 Dataset Characterization

This study's dataset is a time series, a collection of observations made sequentially over regular intervals of time, such as hours, days, weeks, months, or years. Each observation in a time series represents the value of a specific variable at a particular point in time [2]. Time series data can be univariate, meaning that only one variable is being measured, or multivariate, where multiple variables are captured simultaneously. Time series are used in various fields such as medicine, finances, and engineering [9]. Through its analysis, it is possible to extract meaningful information which can be used to make informed decisions, identify patterns and trends, and even develop forecasting models.

In time series, past values may influence future values, and sometimes seasonality and trends might be present in the data [3], which should be captured by the model, therefore, using a simple regression model will not be enough to provide accurate forecasts. Thus it is necessary to be somehow able to train the model with past values, multi-step forecasting solves this problem.

The used dataset is univariate, in which the only available information is the daily transactions in each section. But the initial dataset was disorganized, with many missing values and outliers. Therefore, extracting the largest amount of sequential values for a new dataset was necessary to ensure a clean dataset suitable for training a regression model.

Like that, the dataset comprised 572 values, however, it also contained outliers identified as days when the store was closed. Since the transactions dropped abruptly to zero on those days, it was decided to replace these outliers with the average value for each section.

2.2 Regression methods

In recursive multi-step forecasting, a certain number of past values (called lags) are stored as features used by a regression model to predict the next value. To make a second prediction, the first predicted value will be used as a lag, as described by Fig. 1 [7]. This procedure can be repeated for any desired period. Although the error from past predictions will propagate, it is advisable not to forecast for an extremely large period.

The regression method is used to make predictions or estimates of the value of the dependent variable based on its relationship with independent variables [13].

In this work, a set of regression methods were selected to determine which would present the best performance with the available dataset. The methods used were the following:

- **Random Forest**, consists of an ensemble of decision trees. To make predictions, it obtains the predictions of all individual trees, then it predicts the class that gets the most votes [4].

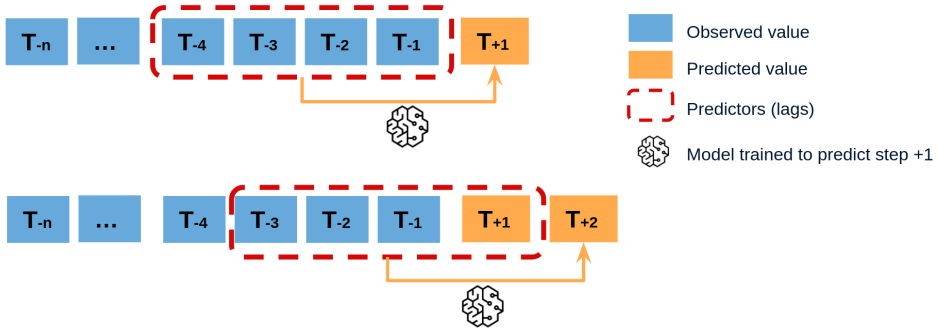


Fig. 1: Recursive multi-step forecasting [7].

- **Gradient Boosting**, relies on an ensemble of decision trees. It works by sequentially adding predictors to an ensemble, each one correcting its predecessor. This method tries to fit the new predictor to the residual errors made by the previous predictor [4].
- **Linear Regression**, is based on fitting the parameters of a straight line to the data via optimization methods. It can be used for univariate or multivariate datasets through the multiple linear regression model [4].
- **Elastic Net**, is a linear regression with a regularization term added to the cost function. This regularization term consists of a mix between Ridge and Lasso regularization which may help the model generalize the model's weight better [4].
- **Bayesian Ridge**, consists of a linear regression with a regularization term determined using Bayesian inference. It helps generalize the model better, thus preventing overfitting [1].
- **Linear Support Vector Regressor**, consists of trying to fit as many instances as possible of data points within the margins of a line while limiting the number of margin violations. The parameters of the line and its margins are adjusted via a quadratic optimizer [4].

The dataset contained 572 sequential days of transaction data for one store. The data set was divided into training (70%) and testing (30%) for the application of regression methods, they were divided this way due to being commonly used in machine learning [4]. The training dataset comprised 400 days and 172 transactions were performed to validate the model's accuracy.

2.3 Error

In Machine Learning, the error provides a metric so that it is possible to evaluate how good a particular model is at making predictions. For this case, it was decided to utilize two different metrics Mean Squared Error (MSE) and Mean Absolute Percentage Error (MAPE). In both these methods, lower values are associated with better predictions.

MSE is calculated by squaring the absolute error. Thus the returned value will always be positive or zero. It can be estimated as described by Equation 1.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2 \tag{1}$$

Y represents the observed value for the period i, $\hat{Y}$ represents the predicted value for the same period, and n is the total periods tested. In MAPE, the error is calculated as in Equation 2.

$$MAPE = \frac{1}{n} \sum_{i=1}^{n} \left| \frac{Y_i - \hat{Y}_i}{Y_i} \right| \tag{2}$$

2.4 Validation

To validate the applied methods, the technique of backtesting with refit was used, which consists of splitting the dataset into 2 parts, the training data and the testing data. The first n values of the testing dataset will be used for validation, corresponding to the number of days to be predicted, the rest of the training dataset will remain unseen [6]. Then the training data amount will increase, the test will decrease by n steps, the model will be retrained, and the validation will be performed. This will happen repeatedly until the end of the dataset is reached [6] as shown in Fig. 2.

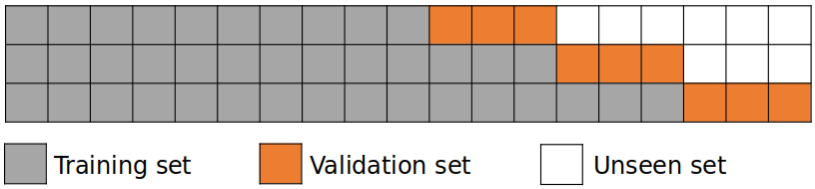


Fig. 2: Example of back-testing with refit [6].

In Fig. 2, it is possible to observe an example of backtesting where one line of squares represent the full dataset. The rows represent each iteration of this method, and the columns represent one observation.

3 Results

The objective of this analysis is to forecast the daily number of transactions executed in 8 sections of a Portuguese retail company store for the next 15 days using historical data.

With the dataset clean and organized, several methods were tested with different amounts of lagged values to evaluate how the model behaved. The backtesting method with refit was used to validate the results for all sections obtaining the MSE and MAPE. As described by Fig. 3 for the butchery section, the MSE is depicted on the left side, while the MAPE is shown on the right. Each row represents a distinct regression model, and each column corresponds to the associated lag for that experiment. The color green indicates lower values, while higher values are represented by the color red. The backtesting method with refit validated the results, obtaining the MSE and the MAPE.

One of the eight sections was chosen for a more detailed demonstration of the results, the butchery section. In Fig. 3, you can see the MSE values on the left side and the

MAPE on the right. Each row represents a different regression model, and each column corresponds to the delay associated with that experiment. The green color indicates lower values, while higher values are represented by red color.

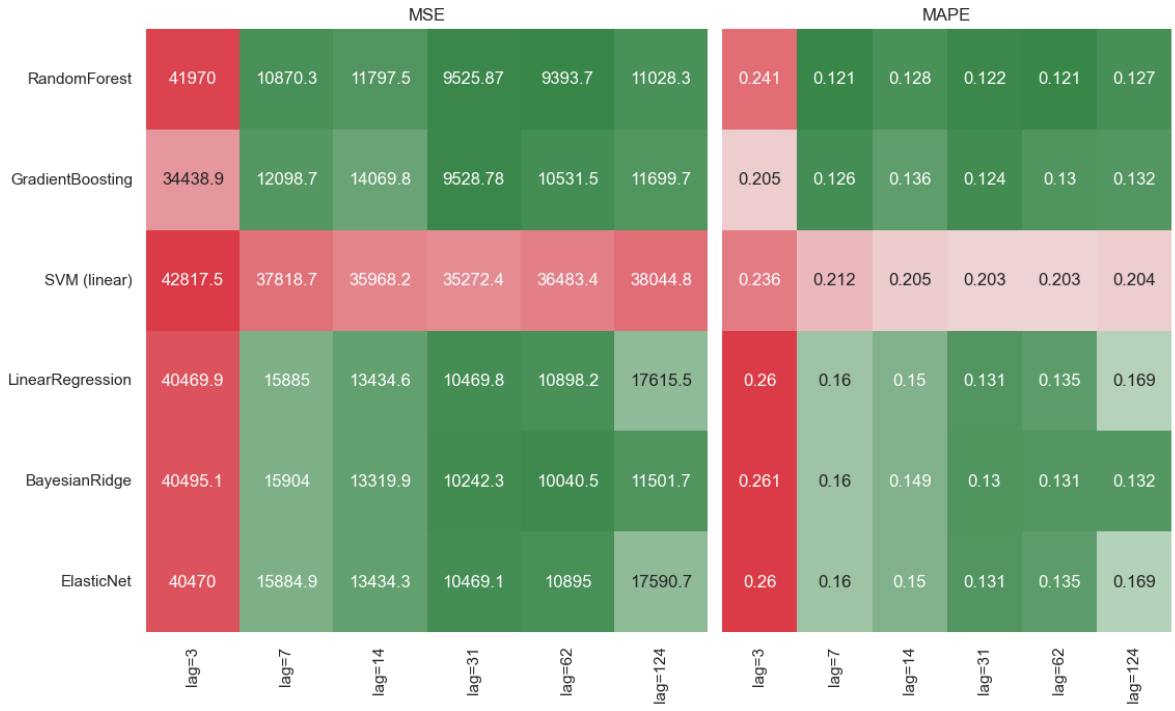


Fig. 3: MSE and MAPE of the validation forecast for the butchery section

From the analysis of the obtained results, it was possible to verify that the best combination of model and amount of lag was the Random Forest algorithm with 62 lag values. This resulted in a MAPE of 12.1% and MSE of 9393.7. Thus, for a better understanding of the results, the predictions made during the backtesting were plotted in a graph, shown in Fig. 4.

By examining Fig. 4 it is possible to observe that the model can predict the transactions performed somewhat accurately. However, it failed to make a reliable forecast in a few days, like 12-03-2022, 09-04-2022, and 17-4-2022 (Easter day), where the number of transactions was not expected.

The same methodology was applied to the other sections. The results are briefly summarized in Table 1 containing only the best-performing model.

It was possible to observe that the model that presented the most accuracy in more sections was gradient boosting, being the best for 4 sections. As for the amount of lag, the best results were presented using 62 for 4 sections and 31 for 3 sections.

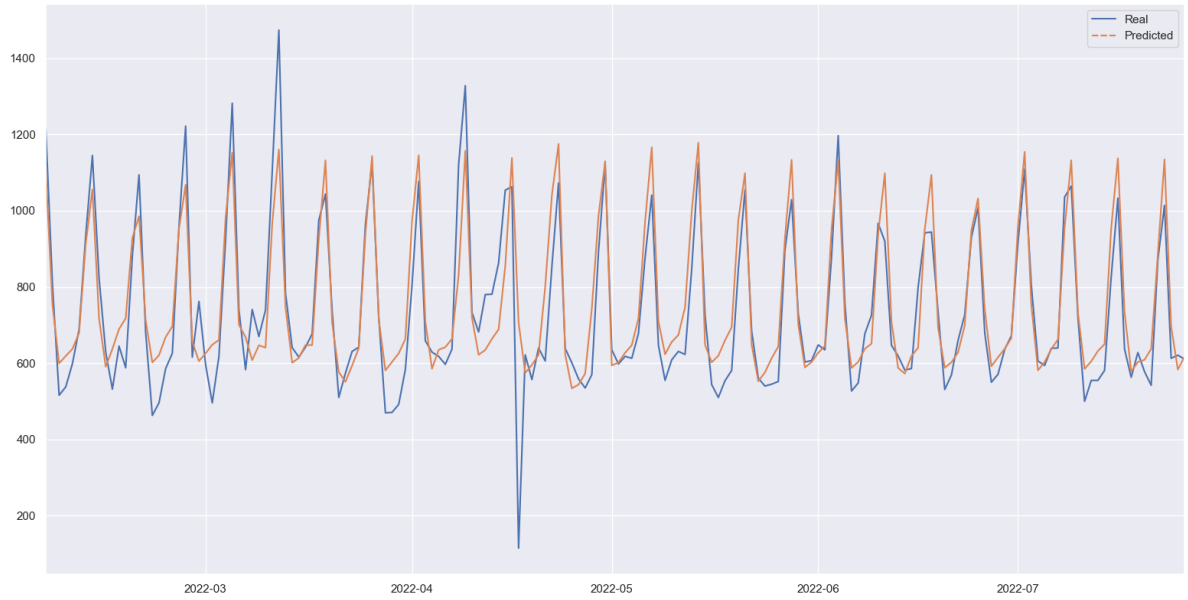


Fig. 4: Plot of the backtesting results for the butchery section forecast with Random forest with 62 lagged values

Table 1: Best performing model for each section of the store

Section	Model	Lag	MSE	MAPE
Butchery	Random forest	62	9393.7	0.121
Fishmonger	Gradient boosting	31	10254.5	0.155
Cheese and charcuterie	Gradient boosting	31	28626.8	0.118
Fruits and vegetables	Gradient boosting	124	29940.3	0.097
Bakery	Gradient boosting	62	29879.7	0.085
Takeaway	Bayesian ridge	62	3751.6	0.085
Non edible	Random forest	31	88452.3	0.118
Textile	Bayesian ridge	62	6856.3	0.167

4 Conclusion and Future Works

It was possible to conclude that regression methods combined with features generated via multi-step forecasting can predict the number of transactions for the different sections of one retail store. However, when the number of transactions abruptly differs from the ordinary amount, the model cannot reliably predict these transactions.

In future works, it is intended to apply this methodology to several stores of the same Portuguese retail company. Subsequently, it is intended to track the expected number of customers through the forecast of transactions and apply this information to the iSafety model. This ongoing project comprises developing a predictive model to calculate the risk of accidents in a Portuguese retail company.

Acknowledgement

The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/ 0007/2021). This work has been supported by NORTE-01-0247-FEDER-072598 iSafety: Intelligent system for occupational safety and well-being in the retail sector.

References

1. Bishop, C.: Pattern Recognition and Machine Learning. Springer, New York, USA (2006)
2. Chatfield, C.: The analysis of time series: An introduction. Chapman & Hall/CRC, Boca Raton, Florida, USA (1995)
3. Grassi, S., Proietti, T.: Stochastic trends and seasonality in economic time series: new evidence from bayesian stochastic model specification search. Empirical Economics **48**, 983—1011 (2014). https://doi.org/https://doi.org/10.1007/s00181-014-0821-y
4. Géron, A.: Hands-On machine learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media, Inc., Sebastopol, California, USA (2019)
5. Li, L.: Workplace safety and worker productivity: Evidence from the miner act. ILR Review **75**(1), 117–138 (2022). https://doi.org/https://doi.org/10.1177/0019793920931495
6. Rodrigo, J., Ortiz, J.: Backtesting forecaster - skforecast docs, `https://skforecast.org/0.4.2/guides/backtesting.html`
7. Rodrigo, J., Ortiz, J.: Skforecast: time series forecasting with python and scikit-learn, `https://www.cienciadedatos.net/documentos/py27-time-series-forecasting-python-scikitlearn.html`
8. Shanti, M.Z., Cho, C.S., Byon, Y.J., Yeun, C.Y., Kim, T.Y., Kim, S.K., Altunaiji, A.: A novel implementation of an ai-based smart construction safety inspection protocol in the uae. IEEE Access **9**, 166603–166616 (2021). https://doi.org/https://doi.org/10.1109/ACCESS.2021.3135662
9. Shumway, R., Stoffer, D.: Time Series Analysis and Its Applications: With R Examples. Springer, New York, USA (2011)
10. Ticona, W., Figueiredo, K., Vellasco, M.: Hybrid model based on genetic algorithms and neural networks to forecast tax collection: Application using endogenous and exogenous variables. 2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON) pp. 1–4 (2017). https://doi.org/https://doi.org/10.1109/INTERCON.2017.8079660
11. Tortorella, G., Cómbita-Niño, J., Monsalvo-Buelvas, J., Vidal-Pacheco, L., Herrera-Fontalvo, Z.: Design of a methodology to incorporate lean manufacturing tools in risk management, to reduce work accidents at service companies. Procedia Computer Science **177**, 276–283 (2020). https://doi.org/https://doi.org/10.1016/j.procs.2020.10.038
12. Vassallo, D., Krishnamurthy, R., Sherman, T., Fernando, H.J.S.: Analysis of random forest modeling strategies for multi-step wind speed forecasting. Energies **13**(20) (2020). https://doi.org/https://doi.org/10.3390/en13205488
13. Weisberg, S.: Applied Linear Regression. Wiley, Hoboken, New Jersey, United States (2014)
14. Zhan, X., Zhang, S., Szeto, W.Y., Chen, X.: Multi-step-ahead traffic speed forecasting using multi-output gradient boosting regression tree. Journal of Intelligent Transportation Systems **24**(2), 125–141 (2020). https://doi.org/https://doi.org/10.1080/15472450.2019.1582950

Using VGs for Feature Selection in Supervised Machine Learning Applied to Detect DDoS Attacks

João Lopes[1], Alberto Partida[2], Pedro Pinto[1,3], and António Pinto[3,4]

[1] Instituto Politécnico de Viana do Castelo, Viana do Castelo, Portugal
jmanuellopes@ipvc.pt, pedropinto@estg.ipvc.pt
[2] Data, Complex Networks and Cybersecurity Sciences Technological Institute, Rey Juan Carlos University, Madrid, Spain
alberto.partida@dcncsciences.com
[3] Instituto Universitário da Maia, Portugal
[4] CIICESI, ESTG, Instituto Politécnico do Porto, Portugal
[5] CRACS & INESC TEC, Porto, Portugal
apinto@estg.ipp.pt

Abstract. The Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are intended to impair the performance of systems and, in extreme cases, lead to their downtime. To detect these attacks, a set of mechanisms can be used such as Machine Learning, namely supervised learning (SL). In this paper, an innovative approach is proposed for selecting the best features using Visibility Graphs (VG) in conjunction with the SL technique to detect DoS and DDoS attacks. The results obtained show that the approach is promising and can lead to further research in this critical area of cybersecurity.

Keywords: Artificial intelligence · Machine Learning · Supervised Learning · Denial of Service attack · Visibility Graph · Cybersecurity.

1 Introduction

Cyber attacks, including denial of service (DoS) attacks, can cause significant financial losses and damage the reputation of affected companies [4, 5]. To detect these attacks, many network-based intrusion detection systems (IDS) are using Machine Learning (ML) algorithms [11].

This article explores the use of Visibility Graphs (VGs) in the feature selection step in Machine Learning (ML) algorithms. VGs are a transformation of time series into complex networks, which offer insights into the underlying dynamics of the data and can be applied in the detection and prediction of anomalies [8]. The objective is to complement, or replace, traditional techniques used in feature selection such as Correlation Analysis, Recursive Resource Elimination, Random Forest or Support Vector Machine (SVM) [1, 2, 7], allowing the ML algorithm to better distinguish DoS attacks from legitimate traffic. This article proposes building VGs to identify, in a fast way, the most informative IP network-related features that would help supervised ML-based Intrusion Detection Systems (IDS) detect DoS attacks.

The remainder of this article is organised as follows. Section 2 provides a detailed review of work related to using ML to detect DoS attacks. The 3 section describes the VGs as well as their capabilities e presents a use case with the proposed idea and the results of the tests carried out. Finally, Section 4 summarizes the main conclusions of this work, discusses the results obtained, and presents directions for future research.

2 Related Work

ML is a field of Artificial Intelligence (AI) that focuses on developing algorithms and models to gain knowledge from data and perform predictions and help decision-making. ML can be categorized into four types based on the learning approach: supervised learning (SL), unsupervised learning, semi-supervised learning, and reinforcement learning [3].

SL is the most prevalent type of ML [12] and involves learning from labeled data, composed of examples of input and their respective outputs, which are used to teach the model to make accurate predictions in future input data. Each input is associated with a known or target output variable. The fundamental steps of SL consist of data preparation, model training, validation, and testing [6].

VGs are intuitive artifacts that transform a time series into a complex connected network. They represent a useful way of studying the underlying dynamics and properties of a time series through the analysis of complex networks. VGs are constructed by converting the time series into a binary sequence based on a previously defined threshold value and then connecting adjacent points above the threshold with undirected edges, forming a graph. VGs have several properties that make them useful for analyzing complex systems, such as freedom of scale, small world, and degree correlation [10, 16].

In this context, visibility networks (VGs) are mathematical graphs that can be easily constructed from time series data to study the underlying properties of the system. Thus, the VGs help analyze data collected from any event in a given time series, and recently it has been used to analyze data and predict future events through mathematical patterns. An example is the use of VG to characterize the contamination of infectious diseases through collected data, intending to predict the number of new infections and the number of hospitalizations and deaths [13]. Another practical case that took advantage of the potential of VG was to evaluate events on the blockchain by analyzing resilience against calculated risks characterized by volatility [14]. And there are many other scientific studies that prove the usefulness of this mathematical tool as well as its advantages. Some of them are the evaluation of time series in a simple way or the possible analysis of patterns, thus creating an event forecasting system. All this added to the low need for processing to perform its tasks, speed, and security.

3 VG and Features Selection in ML

The VGs represent time series and are characterized by a set of points in the Euclidean plane. Their height represents the values of each issue, and the two ends of a series are only related to each other if they are visible to each other through a straight line [9], represented in Figure 1.

To assess the capacity of VGs to aid in the detection of DoS attacks, a use case was built. A DDoS dataset available in Kaggle [15] was selected. This dataset includes 77 resource columns and 1 target column, in *csv* format. Each packet is labeled with a label that differentiates the type of traffic. The following three types are distinguished: *Slow loris DDoS*, *Hulk DDoS*, and *Benign*.

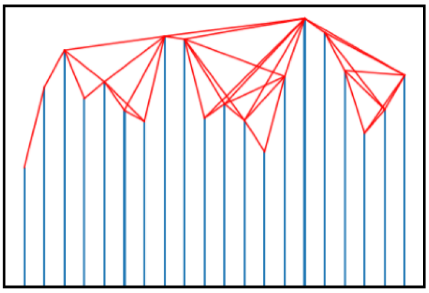


Fig. 1: Example of Visibility Graph

For a better analysis we will use the features highlighted by Ana Sarcevic et al. [17], which used ML to extract information from the dataset, the features obtained, which according to the study, are the best for analysis.

Using the proposed dataset, the analysis focuses on how VGs support the selection of the best input features for ML algorithms in DDoS detection. Table 1 contains two of the best features to detect DDoS attacks and describes the usefulness of the mentioned selected features when building their corresponding VGs based on the study by Ana Sarcevic et al;. [17].

Table 1: Set of the best features for detecting DoS and DDoS attacks, according to [17].

No.	**Feature**	**Description**
1	Init Win bytes forward	The total number of bytes sent in the initial window in the forward direction
2	Flow IAT Mean	Average time between two packets sent in the stream

Figures 2 and 3 present the VGs for the features presented in Table 1. On the left side figure is presented the graphical representation of benign traffic and on the right is the DDoS attack traffic.

By analyzing Figures 2 and 3, it is possible to extract some important details that confirm the usefulness of VGs in this context. Taking into account the study [17] from which these 2 features were extracted, there are details that characterize the type of traffic of each one of them. In table 2 it is possible to verify that all the information obtained through the study goes against the results obtained through the VGs.

Table 2: Usefulness of the selected features provided in [17].

No.	**Feature**	**Info**
1	Init Win bytes forward	High values characterise benign traffic, while low values characterise DDoS attacks.
2	Flow IAT Mean	High values are indicative of DoS attacks, while low values are indicative of benign traffic.

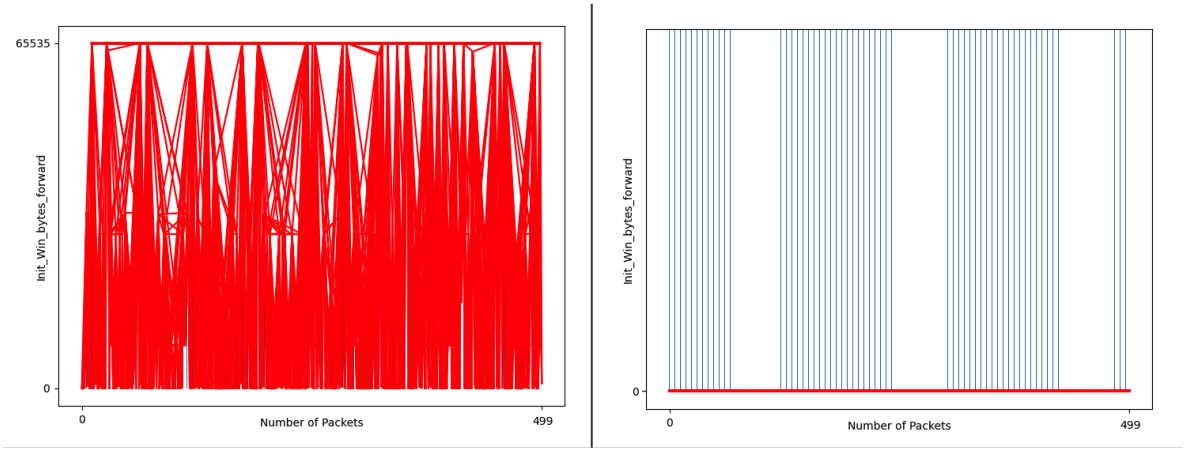


Fig. 2: VGs for feature *Init Win Bytes Forward*

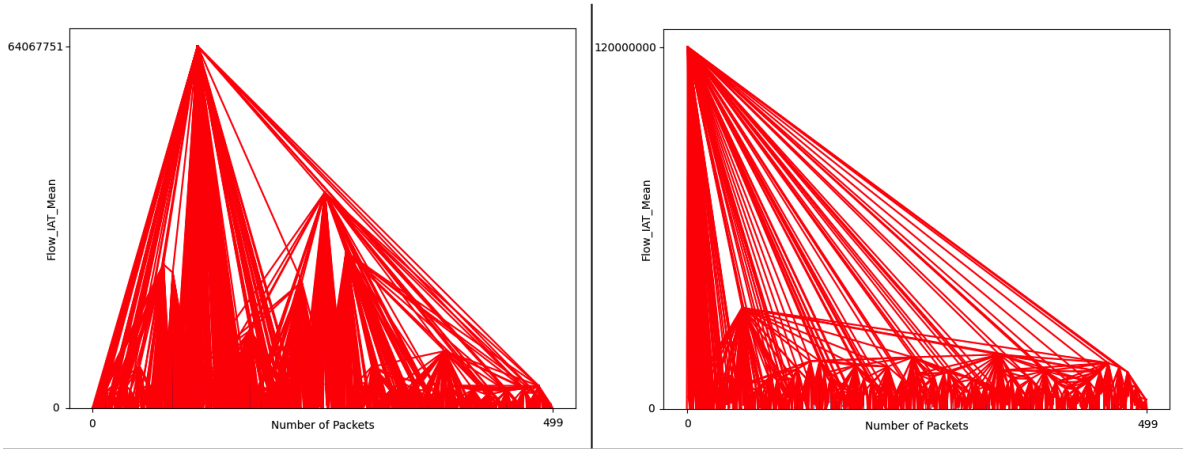


Fig. 3: VGs for feature *Flow IAT Mean*

4 Conclusion

The present article proposes a new approach for supervised machine learning feature selection based on the use of VG and the results are promising: VGs can be considered to aid the stage of features selection techniques in ML.

This proposal has advantages and disadvantages. On the one hand, VGs are easy and fast to implement, require little computational resources, and offer satisfactory results. On the other hand, if the time interval under analysis involves a large amount of data, the computation time to plot the VGs increases linearly.

The results obtained are promising and open doors to new research possibilities in the area. Although the selection of network resources depends on the type of attack analyzed, one can explore the application of this VG-based resource selection technique to identify other types of cyber attacks.

References

1. Abbas, L.B., Sadiq, M.A., Ahmad, M.O.: Machine learning-based detection of ddos attacks: A review. Future Generation Computer Systems **111**, 799–811 (2020)
2. Gani, A., Ullah, S., Khan, K.: Detection of denial of service (dos) attacks using machine learning techniques. In: 2019 International Conference on Computer and Information Sciences (ICCIS). pp. 1–6. IEEE (2019)
3. Goodfellow, I., Bengio, Y., Courville, A.: Deep learning. MIT Press (2016)
4. Gupta, B.B., Badve, O.P.: Taxonomy of dos and ddos attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications **28**(12), 3655–3682 (2017). https://doi.org/10.1007/s00521-016-2317-5
5. Gupta, B., Gupta, R., Tyagi, S.K.: Taxonomy of ddos attacks and their prevention techniques: a review. Journal of Network and Computer Applications **126**, 48–73 (2019). https://doi.org/10.1016/j.jnca.2018.10.009, `https://doi.org/10.1016/j.jnca.2018.10.009`
6. Hastie, T., Tibshirani, R., Friedman, J.: The elements of statistical learning. Springer Science & Business Media (2009)
7. Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M.A., Kim, K.Y.: Detecting ddos attacks with machine learning techniques. Information Sciences **254**, 1–14 (2014)
8. Lacasa, L., Luque, B., Ballesteros, F., Luque, J., Nuno, J.C.: From time series to complex networks: The visibility graph. Proceedings of the National Academy of Sciences **105**(13), 4972–4975 (2008)
9. Lacasa, L., Luque, B., Ballesteros, F., Luque, J., Nuno, J.C.: From time series to complex networks: The visibility graph. Proceedings of the National Academy of Sciences **105**(13), 4972–4975 (2008)
10. Lucas, T., da Fontoura Costa, L., Correa da Rocha, L.E.: Visibility graph analysis: a review. Journal of Statistical Mechanics: Theory and Experiment **2014**(8), 08001 (2014)
11. Mishra, D.K., Singh, V.P., Tripathi, R.: Network security situation awareness using visibility graph. Journal of Network and Computer Applications **58**, 49–62 (2015). https://doi.org/10.1016/j.jnca.2015.09.007, `https://www.sciencedirect.com/science/article/pii/S1084804515001866`
12. Nasteski, V.: An overview of the supervised machine learning methods. HORIZONS.B **4**, 51–62 (12 2017). https://doi.org/10.20544/HORIZONS.B.04.1.17.P05
13. Ni, K., Xu, J., Roach, S., Lu, T.C., Kopylov, A.: Characterizing disease spreading via visibility graph embedding. In: 2021 IEEE International Conference on Big Data (Big Data). pp. 2656–2661 (2021). https://doi.org/10.1109/BigData52589.2021.9671810
14. Partida Rodríguez, A.: Resilience against intentional risk inblockchain implementationsusing complex networks pp. 135–144 (09 2022), `http://hdl.handle.net/10115/20049`
15. Warda: Application-layer ddos dataset. `https://www.kaggle.com/datasets/wardac/applicationlayer-ddos-dataset?select=test_mosaic.csv` (2020)
16. Xiang, J., Small, M.: Visibility graphlet approach to chaotic time series. Physical Review E **92**(6), 062817 (2015)
17. Šarčević, A., Pintar, D., Vranić, M., Krajna, A.: Cybersecurity knowledge extraction using xai. Applied Sciences **12**(17) (2022). https://doi.org/10.3390/app12178669, `https://www.mdpi.com/2076-3417/12/17/8669`