DOI: 10.15439/2023F2510
ISSN 2300-5963 ACSIS, Vol. 35

# Laundry Cluster Management Using Cloud

Mateusz Salach*, Bartosz Trybus†, Bartosz Pawłowicz‡, Marcin Hubacz†
*Department of Complex Systems
0000-0002-9199-3460
Rzeszow University of Technology
al. Powstancow Warszawy 12, 35-959 Rzeszow
Email: m.salach@prz.edu.pl
†Department of Computer and Control Engineering
0000-0002-4588-3973
0000-0002-2748-1145
Email: btrybus@prz.edu.pl, m.hubacz@prz.edu.pl
‡Department of Electronic and Telecommunications Systems
0000-0001-9469-2754
Email: barpaw@prz.edu.pl

***Abstract*—Electronic devices in the 21st century have numerous network components, including wireless or wired Internet access modules. Connecting devices to networks and cloud services enables them to access new functionalities and unlock system updates and device security enhancements. The article presents the concept of an intelligent laundry management system based on RFID and cloud computing. The Internet connection not only unlocks additional features of the washing machine, such as different washing modes, but also allows for selecting the appropriate detergent level and washing parameters based on the textile material being washed. Additionally, the paper presents the solution and measurement studies on the accuracy of textile identification.**

## I. Introduction

Technological development can be observed in many aspects of human life. Modern solutions can be seen all around, for example, controlling home facilities from a smartphone [1], shopping online using a phone, computer, or even autonomously by a refrigerator. The use of technology facilitates work, life, and provides more opportunities for self-focus. Solutions based on the Internet of Things (IoT) are gaining significant popularity, as well as the increasingly popular idea of the Internet of Everything (IoE) [2]. The concept of IoT devices is to establish a stable connection to both home and public computer networks, as well as the cloud, which enables remote administration of the device, whether it's a refrigerator, car, or a home automation system. The wide availability of services and possibilities can influence living conditions if one knows how to use them physically and safely. However, in many cases, the solutions proposed by manufacturers are unsafe [3], [4]. IoT security measures are often minimal, limited to simple mechanisms. Such solutions provide significant opportunities for hackers who can, for example, gain access to a building by attacking a home appliance, thus gaining entry to the main home network. The analysis of IoT devices from a cybersecurity perspective is particularly emphasized in the era of a very large number of IoT devices in residential buildings. Research allows for the detection of new methods of authentication and security measures used in various IoT device [5],[6].

IoT devices are most commonly equipped with WiFi modules or, in the case of specialized devices, Ethernet modules, which, when connected to the global network, unlock additional functionalities. These devices can be based on less advanced controllers such as NodeMCU [7],[8], ESP [9],[10], Raspberry Pi [11], as well as more advanced modules like PLC controllers [12]. Such solutions can utilize artificial intelligence algorithms for efficient management of electricity consumption [13],[14] and [15], or heating systems [16],[17],[18], not only in individual buildings but also in a cluster of buildings managed from the cloud [19],[20] and [21]. Due to the availability of components and a substantial base of online tutorials, it is possible to build custom Smart Home solutions using popular microcontrollers such as Arduino, ESP, etc. However, a key element is securing the entire system against external attacks.

As mentioned, IoT devices unlock most of their functionality through connection to the cloud computing. Devices equipped with a series of cameras can analyze their content and react accordingly, for example, by notifying the user that it's time to go shopping. Cars equipped with temperature sensors can inform the user through a push notification on their phone, via a dedicated application, that the car is heated or cooled and ready to drive. The amount of data required for processing and the memory needed to store the database is often so large that it is impossible to store all the requested information locally. Thus, in the case of many devices working together, the communication requires a connection to the cloud computing in order to properly manage the data exchange.

An example of such a solution can be a system of intelligent washing devices currently under development, as presented in this paper. It is assumed here, that the washing appliances have additional modules that allow for management and adjustment of washing parameters for textile materials using an RFID system. The concept of integrating washing devices with the cloud computing is demonstrated using the example of the Microsoft Azure IoT Hub service and its services, RFID system, and proprietary laundry management software. Research on information reading in washing devices is also presented. The last section summarizes the research results and presents potential paths for the project's development.

## II. Smart Laundry in the Era of IoT and Cloud Computing

Despite the large access to household washing machines, laundries are still popular and used not only for traditional everyday clothes, but especially for textiles that require specialized treatments. Each fabric requires appropriate washing agents to be used without damaging the material. Some clothes require more specific measures, while for others they can be more universal. The idea of an intelligent laundry system is to adapt the chemical agents, their dosage, and grouping based on the fabric inserted into the washing machine.

Considering the wide range of laundry detergents available and the constant emergence of new liquids and powders, storing their information along with the clothing would be an outdated solution. This means that whenever new products appear, the information for each garment would require updating. A much flexible and future-proof solution is to store the data in the cloud, where the database can be updated at any time. This allows for the utilization of products that have recently entered the market in a very short time.

The idea of operation of an intelligent cluster of washing devices is presented in Fig. 1

As seen, each device is equipped with an Ethernet module or a WiFi module for communication with the network. When a washing machine connects to the Internet, it immediately unlocks the connection to the cloud by retrieving necessary data, such as pending software updates, new washing programs. The device may also send data to the manufacturer regarding the current status of the machine or informing the operator about the current washing process. An offline mode must be provided in case of a network connection problem. However, when appropriate fabrics are detected, the offline data is overwritten with information obtained from the cloud.

The RFID (Radio Frequency IDentification) system was used to recognize the textiles. They contain RFID tags with information about the product [22].Typical data is shown in Fig. 2.

The RFID identifier has security keys and a write-lock feature, preventing the introduction of incorrect materials/components into the washing device, thus avoiding damage. An important element is the `Cloth_code` - a special string of characters assigned, for example, by manufacturers during production, confirming that it is a suitable material for washing. This key is verified against a database to confirm the material after reading its content. The UUID serves as a unique product identification number. It can be checked in the database for existence and based on it, the ideal washing conditions can be selected, taking into account the manufacturer's recommendations available in the cloud database. In

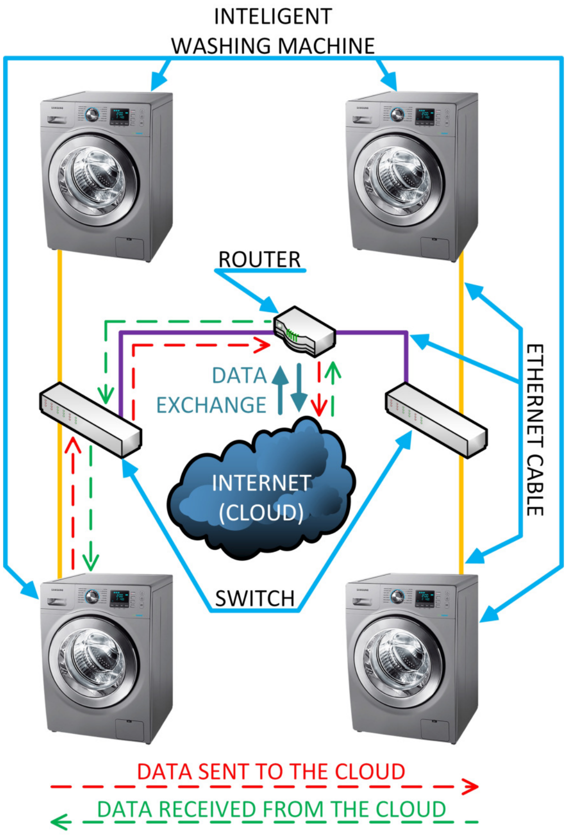

Fig. 1. A cluster of intelligent washing devices

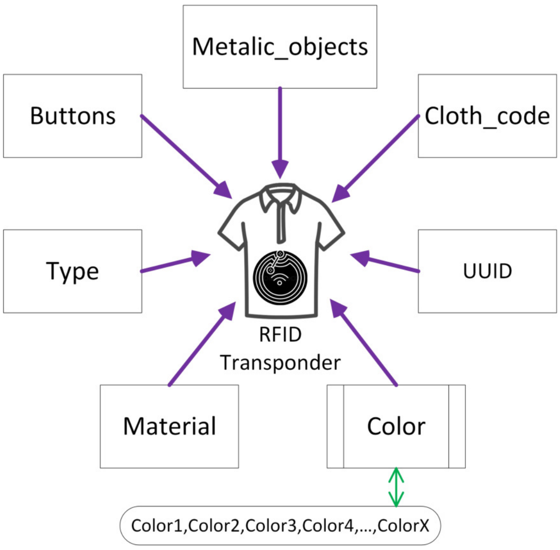

Fig. 2. Data structure in the memory of the RFID identifier

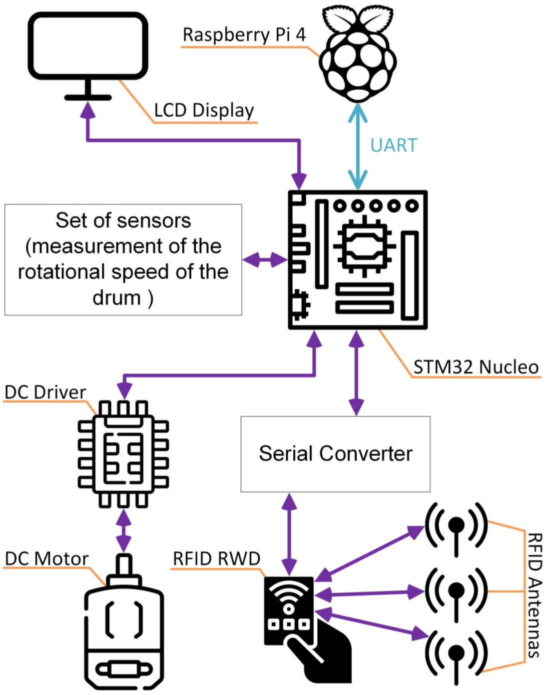

Fig. 3. Diagram of connections and communication between electronic components

the absence of records associated with a particular material, other parameters such as type, fabric, and color are taken into consideration.

To conduct the tests, a device was developed that contains 3 FEIG RFID read/write readers (RWDs). The entire device is controlled using an STM32 microcontroller embedded in the Nucleo board, which features a 32-bit M4 processor with 512KB flash memory and 128KB RAM. The Nucleo board is connected to a touch LCD display, FEIG reading/writing devices, and DC motors for drum rotation control. Since the Nucleo board does not have wireless or wired network modules for internet communication, the Raspberry Pi 4 microcomputer was used. It runs Raspberry Pi OS Lite, which does not have a graphical interface. The Raspberry Pi is connected to the STM microcontroller via the UART interface. The functional diagram is presented in Fig. 3.

After placing clothes equipped with RFID identifiers, the drum rotates to read the data from memory using RWD. In the next step, the information is retrieved and aggregated by a dedicated Python script running on the Raspberry Pi. The data is adjusted accordingly and transmitted to the Azure cloud using Raspberry Pi's wireless (WiFi) or wired (Ethernet) modules.

The project utilized the Azure IoT Hub service, which provides the necessary sub-services to fully leverage the potential of the intelligent cluster of washing machines. In the cloud, the uploaded data is compared with the records in the database, and after successful verification, the device receives instructions on the specific washing parameters for the given fabric. Each incoming data originates from a dedicated device identified by a unique identifier assigned by Azure. This enables the aggregation and processing of a large volume of data from multiple devices simultaneously. When sending data to the cloud, the device must authenticate itself in the service before transmitting any information to the database. To authenticate a device in the cloud, it is necessary to include it in the Azure IoT Hub settings, which will generate the required connection string along with login credentials. Each device is provided with access keys and individual character string, allowing for its identification in the cloud. All steps are presented in the diagram shown in Fig. 4.

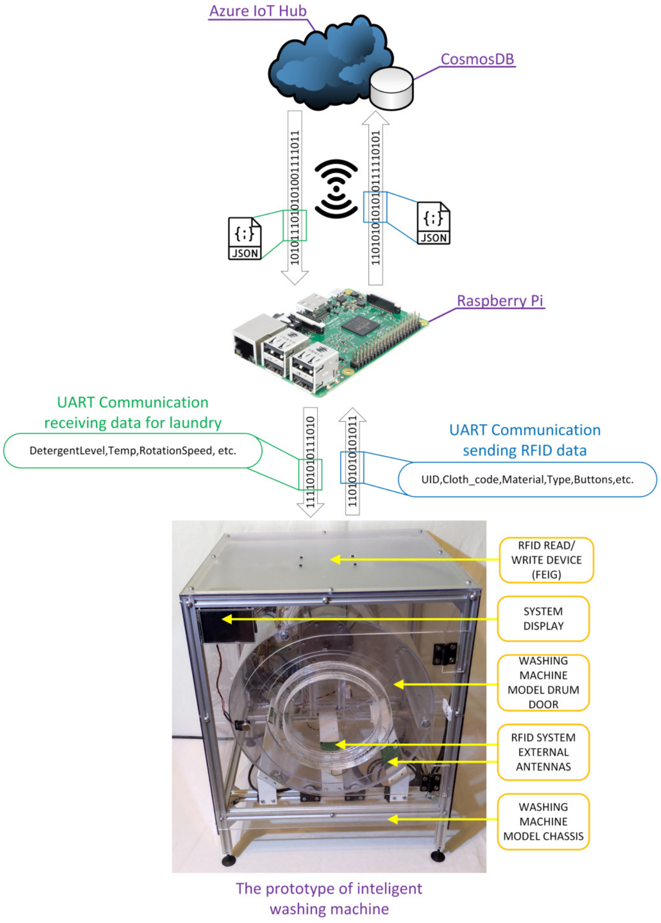
Azure IoT Hub
CosmosDB
1010111101010101001111011
JSON
1101010101010101111110101
JSON
Raspberry Pi
UART Communication receiving data for laundry
DetergentLevel,Temp,RotationSpeed, etc.
1111010101011111010
UART Communication sending RFID data
UID,Cloth_code,Material,Type,Buttons,etc.
11010101010101011
RFID READ/ WRITE DEVICE (FEIG)
SYSTEM DISPLAY
WASHING MACHINE MODEL DRUM DOOR
RFID SYSTEM EXTERNAL ANTENNAS
WASHING MACHINE MODEL CHASSIS
The prototype of inteligent washing machine

Fig. 4. Data transmission between a washing machine and a computing cloud

The data obtained from the cloud computing (Azure IoT service) is transmitted to Raspberry Pi, which modifies the incoming information accordingly. It then sends the information via the UART interface to the STM32 microcontroller, along with laundry-related details such as detergent dosing, drum rotation settings, and the amount of powder to be dispensed. Additionally, the LCD screen displays information related to the recommended detergent and laundry powder provided by the manufacturer.

## III. Reading textile data

As part of the research work, accuracy analyses were conducted on the detected objects in the smart washing device. For this purpose, 30 RFID identifiers simulating clothes were used to determine the number of scans required to correctly read all the identifiers inside the washing machine. The results are presented in Figure 5, divided into the number of scans as 1-3 and 4-6, respectively.

As can be observed in Fig. 5 on the left chart, during a single full drum rotation with the identifier scanning, the accuracy of reading individual identifiers decreases as the number of clothes in the drum increases. In the case of a small quantity of 1-2 clothes, a 100% reading accuracy can be determined. In the range of 3 to 15 identifiers (clothes), the success rate of scanning ranges from 93% to 97%, which seems a pretty good result for a single rotation. Unfortunately, with a larger quantity of clothes, the level of accuracy decreases. This is due errors in reading data from the identifiers or a lack of power supplied to the identifier memory during a single rotation. It is worth noting that the device is equipped with 3 antennas for reading identifiers, which are activated during one rotation, resulting in good reading accuracy even with a large number of clothes.

In the case of two full drum rotations, a significant improvement in reading the fabric information can be observed. The reading accuracy is 100% for a range of 1 to 16 clothes inside the washing machine. The accuracy starts to decrease from 17 clothes, but within the range of 17 to 21 identifiers, the accuracy level still remains above 90%, which is a satisfactory result. The lowest value, 60%, appears only at 30 clothes, whereas in the case of a single rotation, the lowest value appeared at 29 clothes and was 44%.

Another measurement was conducted by performing 3 scans, which means 3 full drum rotations. As can be seen, the measurement accuracy increased for a larger number of clothes. The scanning achieved a 100% value even for 21 RFID identifiers. The accuracy level remained above 90% for 22 and 24 identifiers. In the case of measuring 23 identifiers, the value reached 88%. This may be related to a lack of power supplied to the memory of the RFID identifiers, which reduced the accuracy measurement results. It is worth noting that even for 30 clothes inside the washer, the reading accuracy level was above 70%.

The right chart of figure 5 presents measurements conducted for 4 to 6 drum rotations to verify the influence of rotations on reading accuracy. Although the previous results showed a significant increase in accuracy level, the readings were still below 80% in the most challenging case. As can be observed, the accuracy level for 4 drum rotations, up to 21 clothes, does not deviate from the results presented on the left chart. In the case of values 20-21, there is a slight decrease to approximately 99%. However, it is worth noting the change in reading results for the range of 27-30 clothes. The reading accuracy significantly improved for 4 rotations, resulting in over 80% accuracy for 30 RFID identifiers. For further analysis, two additional scans were conducted, namely 5 and 6 drum rotations. For the 5 scans (5 rotations), another accuracy leap can be observed for the final values. In the case of 30 clothes inside the intelligent washing device, the accuracy level reached over 90%, as well as for all the remaining cases. However, it can be noticed that an increase in the number of drum rotations did not significantly affect the values in the range of 23-26 RFID identifiers. To validate the results, a 6-fold drum rotation was performed, and the results are presented in Fig. 5. It can be observed that the accuracy for 30 clothes did not change significantly, with only a 1% increase. However, the reading levels for the range of 23-28 RFID identifiers slightly improved. The last two scans show that the accuracy level stabilized, and subsequent rotations do not significantly affect the data readings from the memory of the identifiers inside the drum of the device. Additional scans may cause changes at a maximum of 1-2%, which does not bring significant changes considering the lowest value of 92%.

For each identified textile, parameters stored in the Microsoft Azure cloud database are analyzed. Dedicated washing parameters for individual materials are retrieved. Then the data is processed to select the best possible washing agents and recommendations. In the case of a different fabrics inside the washing machine, averaged washing conditions are selected to avoid damaging any of the materials.

## IV. Conclusion

The presented paper showcases a prototype of an intelligent laundry management system connected to the cloud. Parameters and washing configurations are retrieved from the database in the Microsoft Azure service. As part of the research, an analysis of textile recognition accuracy was conducted. This is crucial for washing automation, especially in public laundries, where each fabric should be correctly identified. The analyses demonstrated high accuracy in reading data from the identifiers after performing 5 and 6 scans, which correspond to full drum rotations, at a level exceeding 90%.

In further work, the authors aim to examine the selection of washing parameters for incompatible materials and introduce the ability to adjust material information in the washing machine before starting the washing process. Additionally, they plan to develop a mobile application that allows managing the washing machine, including reading the current materials inside the device. The development of the application will enable further advancement of the project towards an intelligent virtual wardrobe with enhanced material control and storage capabilities.

## Acknowledgment

This project is financed by the Minister of Education and Science of the Republic of Poland within the “Regional Initiative of Excellence” program for years 2019–2023. Project number 027/RID/2018/19, amount granted 11 999 900 PLN.

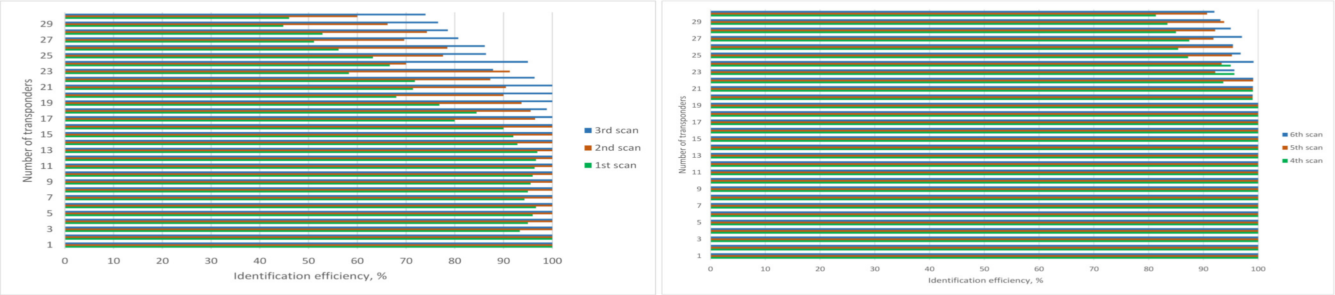

Fig. 5. Reading efficiency of identifiers depending on their number for 1 - 6 scans

## References

[1] K. Rathi, V. Sharma, S. Gupta, A. Bagwari, and G. S. Tomar, “Home Appliances using loT and Machine Learning: The Smart Home,” in *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*. Al-Khobar, Saudi Arabia: IEEE, Dec. 2022, pp. 329–332. [Online]. Available: https://ieeexplore.ieee.org/document/10008294/

[2] O. Ameri Sianaki, A. Yousefi, A. Rajabian Tabesh, and M. Mahdavi, “Internet of everything and machine learning applications: Issues and challenges,” in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2018, pp. 704–708.

[3] A. J. Chinchawade and O. S. Lamba, “Authentication schemes and security issues in internet of everything (ioe) systems,” in *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2020, pp. 342–345.

[4] J. Ryoo, S. Kim, J. Cho, H. Kim, S. Tjoa, and C. Derobertis, “Ioe security threats and you,” in *2017 International Conference on Software Security and Assurance (ICSSA)*, 2017, pp. 13–19.

[5] H. Khalid Alkahtani, K. Mahmood, M. Khalid, M. Othman, M. Al Duhayyim, A. E. Osman, A. A. Alneil, and A. S. Zamani, “Optimal Graph Convolutional Neural Network-Based Ransomware Detection for Cybersecurity in IoT Environment,” *Applied Sciences*, vol. 13, no. 8, p. 5167, Apr. 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/8/5167

[6] H. A. Abdulghani, A. Collen, and N. A. Nijdam, “Guidance Framework for Developing IoT-Enabled Systems’ Cybersecurity,” *Sensors*, vol. 23, no. 8, p. 4174, Apr. 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/8/4174

[7] B. V. Albons, K. H. Yusof, N. H. Mahamarowi, A. S. Ahmad, and A. S. M. Azlan, “Designation of a Home Automation System using Nodemcu with Home Wireless Control Appliances in Traditional Malay House,” in *2022 Engineering and Technology for Sustainable Architectural and Interior Design Environments (ETSAIDE)*. Manama, Bahrain: IEEE, Jun. 2022, pp. 1–3. [Online]. Available: https://ieeexplore.ieee.org/document/9906385/

[8] M. Ibne Joha, M. Shafiul Islam, and S. Ahamed, “IoT-Based Smart Control and Protection System for Home Appliances,” in *2022 25th International Conference on Computer and Information Technology (ICCIT)*. Cox’s Bazar, Bangladesh: IEEE, Dec. 2022, pp. 294–299. [Online]. Available: https://ieeexplore.ieee.org/document/10054941/

[9] M. A. Khan, I. A. Sajjad, M. Tahir, and A. Haseeb, “IOT Application for Energy Management in Smart Homes,” in *IEEC 2022*. MDPI, Aug. 2022, p. 43. [Online]. Available: https://www.mdpi.com/2673-4591/20/1/43

[10] Nur-A-Alam, M. Ahsan, M. A. Based, J. Haider, and E. M. G. Rodrigues, “Smart Monitoring and Controlling of Appliances Using LoRa Based IoT System,” *Designs*, vol. 5, no. 1, p. 17, Mar. 2021. [Online]. Available: https://www.mdpi.com/2411-9660/5/1/17

[11] S. Venkatraman, A. Overmars, and M. Thong, “Smart Home Automation—Use Cases of a Secure and Integrated Voice-Control System,” *Systems*, vol. 9, no. 4, p. 77, Oct. 2021. [Online]. Available: https://www.mdpi.com/2079-8954/9/4/77

[12] S. Subramanian, M. Bindhu, S. Umathe, S. Rao, S. Deivasigamani, and M. Ramarao, “Wireless Sensor & RFID Based Smart Energy Management for Automated Home,” in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*. Trichy, India: IEEE, Nov. 2022, pp. 1125–1129. [Online]. Available: https://ieeexplore.ieee.org/document/10010710/

[13] S. P. Ramalingam and P. K. Shanmugam, “Hardware Implementation of a Home Energy Management System Using Remodeled Sperm Swarm Optimization (RMSSO) Algorithm,” *Energies*, vol. 15, no. 14, p. 5008, Jul. 2022. [Online]. Available: https://www.mdpi.com/1996-1073/15/14/5008

[14] M. Bolanowski, A. Gerka, A. Paszkiewicz, M. Ganzha, and M. Paprzycki, “Application of Genetic Algorithm to Load Balancing in Networks with a Homogeneous Traffic Flow,” in *Computational Science – ICCS 2023*, J. Mikyška, C. De Mulatier, M. Paszynski, V. V. Krzhizhanovskaya, J. J. Dongarra, and P. M. Sloot, Eds. Cham: Springer Nature Switzerland, 2023, vol. 14074, pp. 314–321, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-031-36021-3_32

[15] M. Khan, J. Seo, and D. Kim, “Towards Energy Efficient Home Automation: A Deep Learning Approach,” *Sensors*, vol. 20, no. 24, p. 7187, Dec. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/24/7187

[16] O. Sinkevych, L. Monastyrskyi, B. Sokolovskyi, Y. Boyko, and Z. Matchyshyn, “Estimation of Smart Home Thermophysical Parameters Using Dynamic Series of Temperature and Energy Data,” in *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*. Lviv, Ukraine: IEEE, Jul. 2019, pp. 934–937. [Online]. Available: https://ieeexplore.ieee.org/document/8879944/

[17] V. I. Akimov, E. N. Desyatirikova, A. V. Polukazakov, S. I. Polyakov, and V. E. Mager, “Development and Research of a "Smart Home" Heating Control System,” in *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. St. Petersburg and Moscow, Russia: IEEE, Jan. 2020, pp. 574–580. [Online]. Available: https://ieeexplore.ieee.org/document/9039541/

[18] M. Aibin, “The Weather Impact on Efficient Home Heating with Smart Thermostats,” in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. Edmonton, AB, Canada: IEEE, May 2019, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/document/8861778/

[19] N. Stroia, D. Moga, D. Petreus, A. Lodin, V. Muresan, and M. Danubianu, “Integrated Smart-Home Architecture for Supporting Monitoring and Scheduling Strategies in Residential Clusters,” *Buildings*, vol. 12, no. 7, p. 1034, Jul. 2022. [Online]. Available: https://www.mdpi.com/2075-5309/12/7/1034

[20] M. Bolanowski, A. Paszkiewicz, and A. Kraska, “Integration of the elements of a distributed IT system with a computer network core using island topology,” *Enterprise Information Systems*, vol. 15, no. 10, pp. 1354–1375, Nov. 2021. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/17517575.2020.1790042

[21] Y. He, J. Tian, and Y. Cao, “Intelligent home temperature and light control system based on the cloud platform,” in *2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP)*. Xi’an, China: IEEE, Apr. 2022, pp. 1437–1441. [Online]. Available: https://ieeexplore.ieee.org/document/9778483/

[22] B. Pawłowicz, K. Kamuda, M. Skoczylas, P. Jankowski-Mihułowicz, M. Węglarski, and G. Laskowski, “Identification efficiency in dynamic uhf rfid anticollision systems with textile electronic tags,” *Energies*, vol. 16, no. 6, p. 2626, Mar 2023. [Online]. Available: http://dx.doi.org/10.3390/en16062626