UDC 004.738.5

WIRELESS DEVICES OF THE HOME AUTOMATION SYSTEM WITH WEB APPLICATION CONTROL INTERFACE

***K. O. Plotnikov*[1], *M. O. Fedorenko*[2], *D. G. Karaman*[3]**

[1] *master's student of the Department of Automation and Control in Technical Systems (AUTS), NTU «KhPI», Kharkiv, Ukraine*

[2] *master's student of the Department of Automation and Control in Technical Systems (AUTS), NTU «KhPI», Kharkiv, Ukraine*

[3] *senior lecturer of the Department of Automation and Control in Technical Systems (AUTS), NTU «KhPI», Kharkiv, Ukraine*

Kyrylo.Plotnikov@cit.khpi.edu.ua

Maksym.Fedorenko@cit.khpi.edu.ua

Modern solutions in the field of home system automation are becoming increasingly popular due to the development of Internet of Things (IoT) technologies and wireless communication [3]. The ability to remotely control household devices via a web application built on the Flask [1] and Vue.js [2] frameworks provides users with a high level of convenience and control. The use of modern microcontrollers and wireless technologies enables the creation of energy-efficient and affordable devices for home automation with minimal data transmission delays. However, as an important aspect remains the development of an accessible and easy-to-use interface for the end user, making local web applications based on single-board computers promising solutions for small-scale home networks. The importance of this topic is driven by the need to create reliable and cost-effective solutions that can integrate into a local network and ensure stable operation under limited resources.

Despite numerous advantages, the integration of IoT into automated systems faces several problems and challenges. One of the main issues is ensuring data security. IoT devices often have limited computational resources, making them vulnerable to cyberattacks [4]. Another important issue is the standardization and compatibility of devices. The variety of technologies and protocols used in IoT complicates the integration of different devices and systems, which can lead to inconsistencies in operation and increased development costs.

A wide range of methods is employed to protect automated systems from the described threats. One of the most effective approaches is network segmentation, where production networks are separated from external and corporate networks. This significantly reduces the risks of intruders penetrating the system. The use of firewalls and intrusion detection systems can prevent unauthorized access and promptly detect attempts at attacks [4].

Data encryption is another key protection method, especially in the context of using wireless networks and the Internet of Things (IoT). Encrypting data transmitted between devices greatly reduces the risks of interception and subsequent modification by malicious actors [4].

To minimize risks associated with the human factor, regular training and education of personnel play an important role. Understanding the principles of automated systems and the basics of cybersecurity by employees significantly decreases the likelihood of errors that can lead to equipment malfunctions.

It is necessary to consider the scalability issues of systems. As the number of connected devices increases, the load on the infrastructure and networks grows, requiring the application of new technologies and approaches to data management. It is also important to consider the power consumption of IoT devices, especially in cases where they operate autonomously and are powered by batteries.

The integration of IoT into automated systems is a complex but promising process that requires careful consideration of all aspects—from security and standardization to scalability and energy efficiency.

The project's task is to develop a home automation system controlled via a local web application hosted on a single-board computer (e.g., Raspberry Pi). The system should interact with wireless devices based on ESP32 microcontrollers, using the ESPNOW data transmission protocol [5]. The goal of the project is to create a functional and user-friendly ecosystem of devices that allows for control of lighting, climate, and other aspects of home automation through an intuitive web interface accessible from any device within the local network. The main focus is on data transmission reliability, energy efficiency, and ease of integrating new devices. The system consists of two parts: one is responsible for device communication within the network (Device Network), and the other focuses on device control and scenario creation (Local Server and User). The structural diagram of the system is shown in Fig. 1.

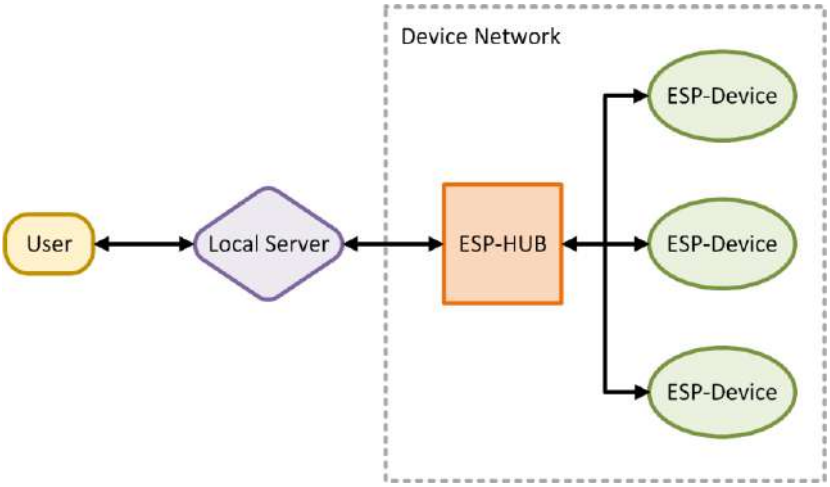

Fig. 1 – Structural diagram of the system

As a result of the work, a system was developed that includes a web application hosted on a single-board computer and a network of ESP32-based devices with ESPNOW support. The web application provides the user with an interface for controlling and monitoring the devices' status in real-time, as well as the ability to configure automation scenarios. The implementation of ESPNOW made it possible to achieve low latency during data transmission and high connection stability between devices without using Wi-Fi. The system demonstrated a high level of energy efficiency due to the minimal power consumption of the ESP32 devices.

List of references:

1. Flask Documentation [Electronic resource]. – Access mode: https://flask.palletsprojects.com/ – As named on title screen.

2. Vue.js Guide [Electronic resource]. – Access mode: https://vuejs.org/guide/ – As named on title screen.

3. *Olivier Hersent*. The Internet of Things: Key Applications and Protocols / *Olivier Hersent, David Boswarthick, Omar Elloumi* // Wiley. – 2012. – 370 p.

4. *Tyson Macaulay*. Cybersecurity for Industrial Control Systems. / *Tyson Macaulay, Bryan L. Singer* // Auerbach Publications, CRC Press, 2011. – 203 p.

5. ESPNOW Overview [Electronic resource]. – Access mode: https://docs.espressif.com/projects/esp-idf/en/stable/esp32/api-reference/network/esp_now.html – As named on title screen.