# Smart and Increased Security Alarm System with Intrusion Detection

Bartha Csaba Richárd
*Obuda University*
*Alba Regia Faculty*
Székesfehérvár, Hungary
bartha.csaba@stud.uni-obuda.hu

Bertalan Beszédes
*Obuda University*
*Alba Regia Faculty*
Székesfehérvár, Hungary
beszedes.bertalan@uni-obuda.hu
https://orcid.org/0000-0002-9350-1802

***Abstract*—This study aims to present a smart alarm system that offers more services than the simple but expensive systems available on the market. It can be developed by users with a smaller financial investment by adding extra functions.**

***Keywords*— smart home, smart alarm system, intrusion sensor, fire alarm, smart switch automation, wifi attack, android hacking**

## I. INTRODUCTION

Nowadays, the need for smart alarm systems is a modern and efficient way to protect our home and property. These systems can identify and report potential dangers, such as fire, burglary, or carbon monoxide leakage, using intelligent sensors and associated devices [1].

Smart alarm systems can be controlled remotely, allowing us to monitor the security of our home anytime, anywhere via a smartphone application [2]. These systems can send quick alerts to the appropriate authorities or the users when events are detected [3]. Intelligent technologies, such as motion detection or face and voice recognition, further enhance the efficiency of these systems [4]. Additionally, smart alarm systems can collect data on security trends and events, helping to predict and prevent potential problems [5].

Overall, these systems contribute to ensuring that our homes and their inhabitants feel safe in the modern world.

## II. THEORETICAL BACKGROUND

The theoretical background of smart alarm systems is closely intertwined with the development of electronics and communication technologies. These systems use intelligent sensors and devices to identify and report potential dangers, such as fire, burglary, or carbon monoxide leakage [6].

The goal of smart alarm systems is to balance security and convenience, allowing users to monitor and control the security of their home or business remotely. These systems are often connected to the internet, enabling users to monitor their home's security live through smartphones or other devices [7].

Smart alarm systems can automatically send alerts to the appropriate authorities or users when suspicious activity is detected. Such systems typically include various sensors, such as motion sensors, door and window sensors, smoke and carbon monoxide detectors, etc. Smart alarm systems play an important role in prevention, as they can provide early warnings of potential dangers. These systems often have sophisticated, cloud-based control and monitoring platforms that allow users to access security-related information about their home from anywhere at any time [8].

Smart alarm systems are generally customizable and expandable, allowing them to adapt to unique needs and changes in the home or business environment. These systems can usually be integrated with other smart home devices, such as smart lighting or smart locks, to provide comprehensive home automation. Smart alarm systems also offer advanced data collection and analysis capabilities, helping users better understand security trends and events affecting their home [9].

Such systems typically have intuitive user interfaces that are easy and efficient to use even for non-technical users. Smart alarm systems often work independently but can cooperate with other home or business automation systems to enhance security and convenience further [10].

## III. CURRENTLY AVAILABLE SOLUTIONS ON THE MARKET

There are numerous solutions on the market in the field of smart alarm systems that allow users to monitor and control their home security remotely.

### *A. Some popular types and services of smart alarm systems*

Many companies offer additional devices that can upgrade traditional alarm systems to smart ones. These typically connect to the Wi-Fi network, allowing users to access them remotely via mobile applications or online platforms [11].

Smart home security systems include devices such as smart cameras, motion sensors, door and window sensors. These devices detect movement and send notifications to users, allowing remote monitoring [12].

Many smart alarm systems are integrated with cloud-based services. This allows storing events and data in the cloud and enables users to access and manage their data from any device [13].

Smart alarm systems are generally accessible through mobile applications. These applications allow users to arm and disarm the alarm system remotely and monitor events.

Smart alarm systems are often capable of cooperating with other smart home devices, such as smart lighting, smart locks, or smart thermostats. This allows users to achieve comprehensive home automation.

It is essential to ensure that the chosen system meets individual needs and expectations. It is always worth thoroughly reviewing the products and consulting with experts or those who have already used similar systems if necessary.

### *B. Purchase prices and differences in unique functionalities*

Smart alarm systems are often offered in different packages. Basic packages generally include fewer sensors and basic services, while extended packages contain more sensors, cameras, and advanced functions. The type of package significantly affects the price.

The more sensors, cameras, and other smart devices are included in the system, the higher the price can be. The increase in price is usually proportional to the expanded functionality and coverage of the system.

If the system offers cloud-based services, such as storing events in the cloud or remote access, this can also affect the

price. Cloud-based services help ensure the secure storage and accessibility of your data.

If the smart alarm system is easily integrable with other smart home devices, such as smart locks, smart lighting, or smart thermostats, the price may increase. However, such integrations can result in more comprehensive home automation.

Smart alarm systems are generally accessible through mobile applications. If the applications are modern and offer comprehensive control and notifications, this can also increase the price.

### *C. Interface options for smart alarm systems*

Smart alarm systems generally come with mobile applications that allow users to monitor and control the system remotely. Applications are usually available on iOS and Android platforms. Many smart alarm systems also have web interfaces, enabling management on desktop or laptop computers. Some smart alarm systems support voice control, allowing users to control the system with voice commands. Certain types of smart alarm systems may include a touchscreen panel or physical control unit for on-site management.

Systems can send email or SMS notifications to users about events detected by sensors. Smart alarm systems often connect to the cloud, allowing users to remotely monitor events and configure the system from any internet-connected device.

Smart alarm systems are generally capable of integrating with other smart home devices, such as smart lighting, smart locks, or smart thermostats. Special interfaces are available for installers and professionals for the installation, configuration, and maintenance of the system. Combining these interfaces, smart alarm systems allow users to manage the system conveniently and efficiently and monitor their home's security.

## IV. SMART ALARM CENTER

### *A. Structure of the smart alarm center*

SONOFF relays operate on a 230V mains power supply, connected with each other by wires as shown in the diagram below (Fig. 1.). The ultrasonic motion sensor is wired to the relay that performs the motion detection function. The relays wirelessly connect to the local network router, allowing remote control via the eWeLink mobile application. The relay performing the siren function wirelessly connects to the network and is wired to the siren.

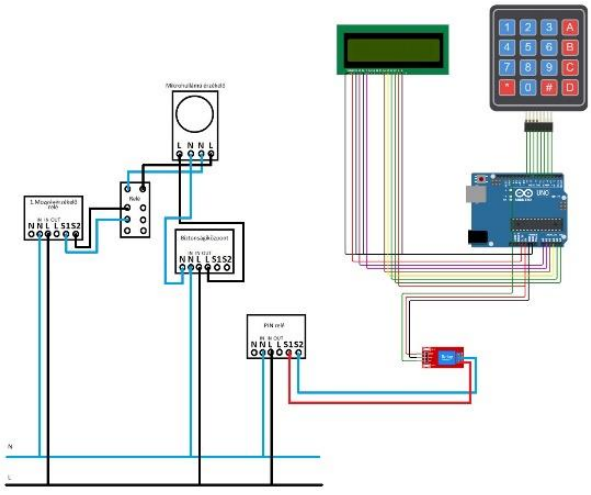

Figure 1: The schematic wiring diagram of the system

When the motion sensor detects movement, the relay performing the motion detection function is activated. When the motion detection relay is ON, and the Security System relay is also ON, the siren relay is activated, and the siren sounds. When the Security System relay is OFF, the motion detection relay loses its power supply, so the motion sensor cannot activate the motion detection relay upon detecting movement. The main flowchart can be seen on Fig. 2.

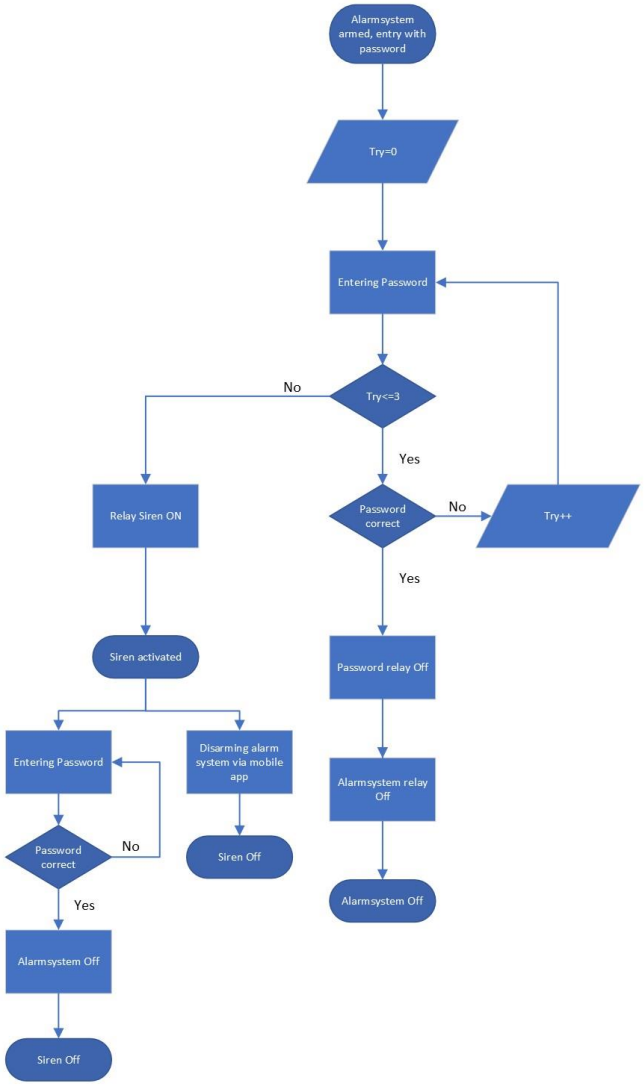


Figure 2: Flowchart of the alarm system

### *B. Arming the alarm system*

Implementing a program code that allows processing, memorizing/storing a given password/code. For PIN code access, I used an Arduino Uno, an LCD display, and a membrane keypad.

The Security System (relay) is not armed (OFF):

After entering the correct PIN code, the display shows "ACCESS GRANTED press # to close", and pressing the # button activates the relay, arming the system, thereby turning on the SONOFF (PIN) wireless relay. The activated PIN relay turns on the SONOFF (security center) relay.

In the eWeLink application installed on the mobile phone, set the "Security Center" switch to ON, and the pre-configured smart control will also turn on the PIN relay (Fig. 3).

If motion is detected, the motion detection relay switches to ON, and the pre-configured smart control will also turn on the siren relay, causing the siren to sound (Fig. 4.).

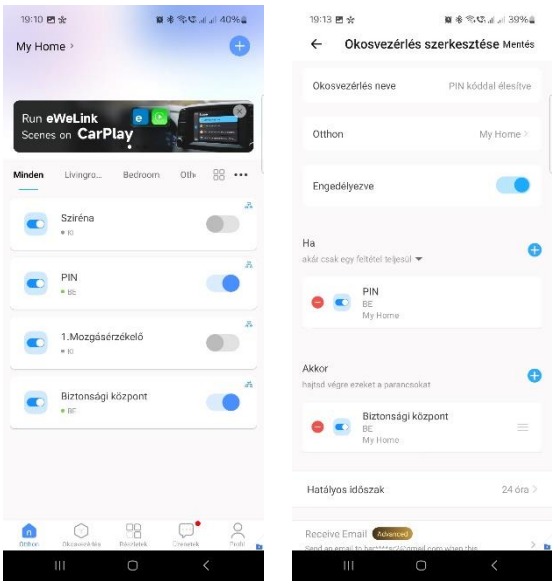


Figure 3: Setting up the application of the alarm system

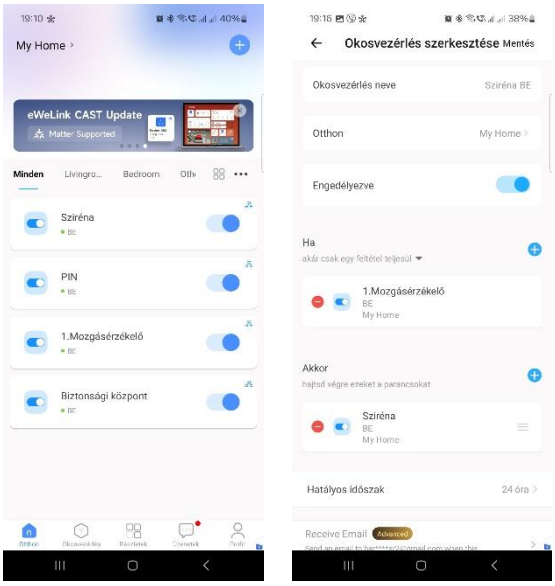


Figure 4: Modifying and testing the alarm system

### C. *Disarming the alarm system can be done in two ways*

Entering the correct password disarms the alarm system (disarming with a keypad). There are 30 seconds to enter the correct code and three attempts; if time runs out or three unsuccessful attempts occur, the system locks, indicating a "burglary," the siren relay switches to ON, and the siren sounds.

Switching the Security Center to OFF in the application also disarms the system.

The application provides real-time information about all Wi-Fi relays and notifies our mobile phone of any status changes. In the mobile phone, we can link the application with the Alexa Assistant and Google Home Assistant applications.

The prototype contains the following modules: Arduino Uno, 16x2 Character LCD display module with blue backlight, 4x4 membrane keypad, Sonoff mini switch, Optonica microwave motion sensor and a 12V siren, see at Fig. 5.

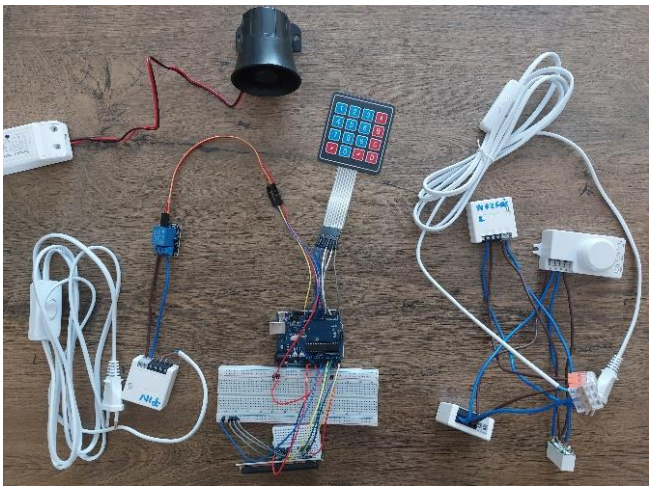

Figure 5: Prototype of the alarm system

## V. THEORETICAL BACKGROUND AND SECURITY ISSUES OF SMART ALARM SYSTEMS

Smart alarm systems are based on various sensors that monitor the home environment and send alerts to the user or a security service when suspicious activity is detected. These systems typically consists sensors, central unit and communication interfaces [14-17].

Motion sensors, door and window opening sensors, smoke and heat detectors can be used. The central unit is the brain that collects data from the sensors and sends alerts. The communication module ensure data transmission between the sensors and the central unit, as well as remote access for users (e.g., via a smartphone application).

Similar hardware close, microcontroller based firmware solutions can be seen in [18-21]. The microcontroller-based solutions presented here can also be applied well in technical frontier areas [22, 23].

### A. *Sabotage possibilities and risks*

The physical sabotage is a physically damaging or anunauthorised access to the alarm system devices. Software sabotage is hacking the system software or installing malicious software.

As a Protective measures, using sabotage sensors can detect physical manipulation or attempts. Secure installation also can help, it is about placing devices in hard-to-reach locations and physically protecting them. Regular software updates and applying security patches and implementing multiple security mechanisms, such as firewalls, antivirus programs, and intrusion detection systems will increase the resistence against software sabotage.

Communication between all elements of the smart alarm system must be reliable and secure. It is proposed to regularly checking the system to ensure all elements function correctly, also setting up automatic notifications and alerts for errors, intrusion attempts, or other suspicious activities [24, 25]. The proposed solution is well suitable for other applications in the term of safety data acquisition [26, 27].

### B. *Loss of connection between modules*

The loss of connection between modules in the alarm system presents several risks. Firstly, the efficiency of the system may decrease if the connection between different modules is lost. This can lead to significant notification gaps,

where alerts may not reach the user or the security service in a timely manner.

To mitigate these risks, several protective measures can be implemented. Utilizing redundant communication channels, such as Wi-Fi and mobile networks, ensures that if one channel fails, the other can maintain the connection. Additionally, conducting regular automatic system checks can immediately notify the user of any connection loss. Setting up outage alerts can also provide warnings about connection loss or communication problems between modules, helping to maintain the overall reliability and effectiveness of the alarm system.

### *C. Smart devices associated with the system's security*

The security of smart devices like phones, laptops, Wi-Fi networks, and assistant services is crucial, as intruders can potentially access the alarm system through these devices. Several risks are associated with compromised smart devices. Firstly, there is the risk of personal data compromise, where intruders can steal or manipulate personal data stored on these devices. Secondly, there is the risk of remote control compromise, where hackers can take control of smart devices remotely.

To protect against these risks, several measures should be implemented. Ensuring device security involves setting up safe configurations for smart devices, such as using screen locks, strong passwords, and regularly updating software. Protecting the Wi-Fi network with strong passwords and encryption is also essential. Additionally, smart assistant services should be properly configured with appropriate access permissions and privacy settings to enhance security.

### *D. Major security risks*

Several major security risks threaten smart home security systems. One significant risk is signal jamming, where hackers can jam wireless signals, interrupting communication between sensors and the control panel. This can significantly compromise the effectiveness of the security system.

Another critical risk is network access. If a hacker gains access to the Wi-Fi network, they can control connected smart devices, including cameras and smart locks, posing a severe security threat.

Device hacking is also a major concern. Poorly protected devices, especially those using default or weak passwords, can be easily hacked. This allows intruders to control the devices remotely and bypass security measures.

Lastly, software and firmware exploitation poses a significant risk. Many smart devices run outdated software or firmware with unpatched security vulnerabilities. Hackers can exploit these weaknesses to gain control over the devices, further compromising the security system.

### *E. Protective measures*

Each device should have strong, unique passwords, means avoid default passwords and change them regularly. It is possible to use a password manager to handle complex passwords.

Using WPA2 or WPA3 encryption on the router secures the Wi-Fi network. Recommended to set a strong Wi-Fi password and considering creating a separate network for smart devices to isolate them from other devices.

Proposed to keep all smart devices updated with the latest software and firmware updates to patch security vulnerabilities and enable automatic updates if possible.

Enable two-factor authentication for smart home applications and accounts adds an extra layer of security in addition to the password.

It is proposed to regularly check the network for unauthorized devices and to use network management tools to see what devices are connected and remove unknown ones.

Good practice to purchase smart devices from reputable manufacturers who prioritize security and provide regular updates. Also to research and read reviews to ensure the devices have a good security track record.

## VI. PRACTICAL IMPLEMENTATION

In the project, the Sonoff relays and the microwave motion sensor power wires are wired to each other. The router provides access to the network through a wireless connection with WPA2 encryption. In case of internet outage, the system cannot be controlled remotely; it continues to operate within the local network, and the application on the remote device will indicate offline status. The armed system can still be disarmed with the Arduino Uno-controlled keypad using a PIN code, and if the mobile device connects to the router's wireless network, it can also be disarmed from the application.

In the event of a router "freeze," using the keypad ensures the on-site activation and deactivation of the system.

The access and privacy settings of the assistant on the mobile device have been configured to avoid hacker attacks.

To calculate the annual energy consumption, check the consumption of the following devices:

1) Sonoff Mini relay:
   - Standby consumption: 0.5W
   - Operating consumption: 1.5W (maximum)
2) Optonica microwave motion sensor:
   - Consumption: approx. 0.5W
3) Arduino Uno:
   - Average consumption: approx. 0.5W

### *A. Annual consumption*

Consumption for all devices in standby mode:

- Sonoff Mini (3 pcs): 1.5W
- Optonica motion sensor: 0.5W
- Arduino Uno: 0.5W

The total consumption in standby mode is:

$$1.5W + 0.5W + 0.5W = 2.5W \quad (1)$$

Consumption for all devices in operating mode:

- Sonoff Mini (3 pcs): 4.5W
- Optonica motion sensor: 0.5W
- Arduino Uno: 0.5W

The total consumption in operating mode is:

$$4.5W + 0.5W + 0.5W = 5.5W \quad (2)$$

Annual energy consumption in standby mode, based on formula (1):

$$2.5W \text{ x } 24 \text{ hours x } 365 \text{ days} = 21.9kWh \quad (3)$$

Annual energy consumption in standby mode, based on formula (2):

$$5.5\text{W x } 24 \text{ hours x } 365 \text{ days} = 48.18\text{kWh} \quad (4)$$

### B. Annual cost

If the local electricity price is approx. 38 HUF/kWh, then the annual cost in standby mode, based on formula (3):

$$21.9\text{kWh x } 38 \text{ HUF/kWh} = 832 \text{ HUF} \quad (5)$$

and in operating mode, based on formula (4):

$$48.18\text{kWh x } 38 \text{ HUF/kWh} = 1830 \text{ HUF} \quad (6)$$

In an average household, the estimated average annual consumption is: 45kWh = 1710 HUF

This summary shows that the annual energy consumption and cost of three Sonoff Mini relays, one Optonica microwave motion sensor, and one Arduino Uno are low, providing an energy-efficient solution for smart homes.

### C. System uptime in case of power outage using an uninterruptible power supply

To calculate uptime during a power outage, consider the system's energy consumption and the UPS battery capacity.The system uses a CyberPower BU650E uninterruptible power supply with a capacity of 12V 7Ah, which equals approximately 84 Wh.

In standby mode, the total consumption is 2.5 W, resulting in an uptime of 33.6 hours (calculated as 84Wh divided by 2.5W). In operating mode, the total consumption is 5.5 W, resulting in an uptime of 15.27 hours (calculated as 84Wh divided by 5.5W).

For summary, the CyberPower BU650E can typically operate the system for approximately 30-35 hours during a power outage.

## CONCLUSION

In conclusion, this study successfully demonstrates the potential of a smart alarm system that surpasses the functionalities of existing market offerings while remaining financially accessible. By enabling users to customize and expand the system with additional features, this innovative approach addresses both cost-efficiency and functionality.

The proposed system not only serves as a viable alternative to expensive commercial options but also empowers users to tailor their security solutions according to their specific needs.

Future work will focus on refining the system's capabilities, enhancing user-friendliness, and conducting extensive field testing to ensure reliability and effectiveness. This development marks a significant step forward in making advanced security systems more accessible and versatile for a broader audience.

## ACKNOWLEDGMENT

The author would like to thank all the Obuda University Alba Regia Faculty staff and member that provide help and assistance throughout the project completion.

## REFERENCES

[1] Javale, Deepali, et al. Home automation and security system using Android ADK. International journal of electronics communication and computer technology (IJECCT) 3.2 (2013): 382-385.

[2] Chen, Joy Iong Zong. "Smart security system for suspicious activity detection in volatile areas." Journal of Information Technology 2.01 (2020): 64-72.

[3] VIDYAVIHAR, MUMBAI. "Remote Controlled Home Automation Using Android Application via WiFi Connectivity." International Journal on Recent and Innovation Trends in Computing and Communication 3.3 (2015): 1489-1492.

[4] Shah, Rakshit, et al. "Wireless smoke detector and fire alarm system." International Research Journal of Engineering and Technology (IRJET) 6.1 (2019): 1407-1412.

[5] Bertalan, Beszédes. Reliable Presence and Intrusion Detection with Collaborative Sensor Modules in Electronic Property Protection Systems. In: IEEE (szerk.) 2019 IEEE 17TH World Symposium on Applied Machine Intelligence and Informatics (SAMI 2019). Herlany, Szlovákia : IEEE (2019) pp. 354-360. , 7 p.

[6] Abdelouahid, R.A., Debauche, O., Marzak, A.: Internet of things: a new interoperable IoT platform. Application to a smart building. Proced Comput Sci 191, pp. 511–517 (2021)

[7] Vadakkan, Annmary, et al. "Door locking using keypad and ARDUINO." International Research Journal of Modernization in Engineering Technology and Science 3.11 (2021): 780-787.

[8] Orji, E. Z., U. I. Nduanya, and C. V. Oleka. "Microcontroller Based Digital Door Lock Security System Using Keypad." International Journal of Latest Technology in Engineering, Management & Applied Science 8.1 (2019): 92-97.

[9] George, Abin. "Automation Of Main Gate, Garage Door and Washing System."

[10] Iqbal, Muhammad Javed, et al. "Smart home automation using intelligent electricity dispatch." Ieee Access 9 (2021): 118077-118086.

[11] Aung, May Aye Chan, and Khin Phyo Thant. IEEE 802.11 attacks and defenses. Diss. MERAL Portal, 2019.

[12] Daniyar Kaliyev, Olga Shvets, György Györök. Computer Vision-based Fire Detection using Enhanced Chromatic Segmentation and Optical Flow Model. Acta Polytechnica Hungarica Vol. 20, No. 6, 2023. ISSN: 1785-8860

[13] Misra, Anmol, and Abhishek Dubey. Android security: attacks and defenses. CRC Press, 2013.

[14] Mosavi Amirhosein, Bertalan Beszedes, Imre Felde, Nadai Laszlo, Gorji Nima E. Electrical characterization of CIGS thin-film solar cells by two- and four-wire probe technique. MODERN PHYSICS LETTERS B 2020 p. 2050102 , 16 p. (2020)

[15] György Györök, Baklanov Alexander E, Bertalan Beszédes. Extension of Nodal Voltage Method with the Thermosensing. In: Orosz, Gábor Tamás (szerk.) AIS 2017 - 12th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2017 by Óbuda University : Proceedings. Székesfehérvár, Magyarország : Óbudai Egyetem (2017) 204 p. pp. 201-204. , 4 p.

[16] György Györök, András Dávid, Nikoletta Tolner, Bertalan Beszédes, Dániel Cseh. Supervision of the operation of digital circuits by Embedded Microcontroller. In: Orosz, Gábor (szerk.) AIS 2018 - 13th International Symposium on Applied Informatics and Related Areas. Székesfehérvár, Magyarország : Óbudai Egyetem, Alba Regia Műszaki Kar (2018) pp. 29-35. , 7 p.

[17] Györök György, Tihomir Trifonov, Alexander E. Baklanov, Bertalan Beszédes, Svetlana V. Grigoryeva, Aizhan Zhaparova. A Special Robust Solution for Battery Based Power Supply. In: Orosz, Gábor Tamás (szerk.) 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország : Óbudai Egyetem (2016) pp. 32-35. , 4 p.

[18] Attila Sáfár, Bertalan Beszédes. Educational Aspects of a Modular Power Management System. In: Orosz, Gábor Tamás (szerk.) AIS 2019 : 14th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2019 by Óbuda University. Székesfehérvár, Magyarország : Óbudai Egyetem (2019) pp. 163-166. , 4 p.

[19] György Györök, Bertalan Beszédes. Artificial Education Process Environment for Embedded Systems. In: Orosz, Gábor Tamás (szerk.) 9th International Symposium on Applied Informatics and Related

Areas - AIS2014. Székesfehérvár, Magyarország : Óbudai Egyetem (2014) pp. 37-42. , 6 p.

[20] Alexander Baklanov, Svetlana Grigoryeva, György Györök. Control of LED Lighting Equipment with Robustness Elements, Acta Polytechnica Hungarica (1785-8860 1785-8860): 15 3 pp 105-119 (2016)

[21] G. Gyorok and M. Mako, "Configuration of EEG input-unit by electric circuit evolution," 2005 IEEE International Conference on Intelligent Engineering Systems, 2005. INES '05., Spain, 2005, pp. 255-258, doi: 10.1109/INES.2005.1555168.

[22] Aizhan Zhaparova, Dimitry Titov, Alexander Y. Baklanov, Gyorgy Gyorok. Study of the Effectiveness of Switching-on LED Illumination Devices and the Use of Low Voltage System in Lighting. Acta Polytechnica Hungarica (1785-8860 1785-8860): 12 5 pp 71-80 (2015)

[23] Thermo-dynamic Cycle Computation of a Micro Turbojet Engine. Fozo, L; Andoga, R and Kovacs, R. 17th IEEE International Symposium on Computational Intelligence and Informatics (CINTI). 2016 17TH IEEE International Symposium on Computational Intelligence and Informatics (CINTI 2016) , pp.75-79

[24] Ediboglu Bartos Gaye, Akyol Serel. Deep Learning for Image Authentication: A Comparative Study on Real and AI-Generated Image Classification. In: Petőné Csuka, Ildikó; Simon, Gyula (szerk.) AIS 2023 - 18th International Symposium on Applied Informatics and Related Areas – Proceedings. Székesfehérvár, Magyarország : Óbudai Egyetem (2023) 177 p. pp. 23-27. 5 p.

[25] Majnár Csaba, Rádli Ferenc Gábor, Ediboglu Bartos Gaye. Augmented Reality in High School Literature: Enhancing Engagement and Evaluation. In: Petőné Csuka, Ildikó; Simon, Gyula (szerk.) AIS 2023 - 18th International Symposium on Applied Informatics and Related Areas – Proceedings. Székesfehérvár, Magyarország : Óbudai Egyetem (2023) 177 p. pp. 155-158. 4 p.

[26] T., Jancso ; A., Podor ; E., Nagyne Hajnal ; P., Udvardy ; G., Nagy ; A., Varga ; Q., Meng ; L., Zhang. Data Integration with Geographic Information System Tools for Rural Environmental Monitoring. In: IRC 2022 XVI. International Research Conference Proceedings. Peking, Kína (2022) 270 p. pp. 52-59. , 8 p.

[27] Peter, Udvardy; Levente, Dimen; Gergely, Vakulya. Data Collection In The Wild: Challenges And Solutions. University of Agronomic Sciences and Veterinary Medicine of Bucharest. Scientific Papers. Series E. Land Reclamation, Earth Observation And Surveying, Environmental Engineering 12 pp. 167-175. , 9 p. (2023)