*Information System and Smart City 2023; 3(1): 528.*
Original Research Article

# On the issue of ensuring the safety of objects with "smart habitat"

**Gennady Dik, Alexander Bogdanov, Nadezhda Shchegoleva, Aleksandr Dik*, Alexander Degtyarev**

*St. Petersburg University, Universitetsky pr., 35, Peterhof, 198504 St Petersburg, Russia*

*** Corresponding author:** Aleksandr Dik, a.dik@spbu.ru

**ARTICLE INFO**

Received: 1 February 2024
Accepted: 29 March 2024
Available online: 9 April 2024

doi: 10.59400/issc.v3i1.528



**ABSTRACT:** The problems of ensuring the security of the smart ecosystem are considered, and an analysis of modern Internet of Things (IoT) devices used in the control loop of the smart habitat is carried out from the point of view of the possibility of protecting and depersonalizing the information circulating in it. The article pays special attention to the issue of integrating a specialized software platform into the smart environment infrastructure, which allows for a high level of not only IT security but also the overall security of the facility. It made an analysis of economic development and subsequent application of the integrated STB platform. Practical recommendations of the organization to improve the security of using the Internet of Things in ODR are considered.

***KEYWORDS:*** smart habitat (SH); Internet of things (IoT); smart infrastructure; artificial intelligence (AI); security and safety system (SSS); smart environment; IT security

## 1. Introduction

Despite some general decline in the market of so-called smart devices to 871.7 million units worldwide (the market for smart home devices in 2022–2023 "sank" by 2.6% compared to the pandemic period[1]), there is a steady increase in interest in smart living systems. According to research and markets[1], the active implementation of deep learning and artificial intelligence and the emergence of more and more smart cities around the world create opportunities for market growth. On the other hand, issues related to information confidentiality and overall security at SH facilities may negatively impact market growth. In this regard, various variants of the security and safety system have recently been increasingly integrated into smart systems.

Typically, such SSS fragments combine many of the functions of a traditional fire and security alarm with the ability to monitor, control, and interact with smart systems from an application on a smartphone, computer, or a special remote control. A smart environment security system is a collection of Internet-connected security devices (IoT devices or, at best, specialized hardware) that typically include a combination of wireless security cameras, sirens, motion detectors, door locks, and sensors that detect when the door or window is open, fire detectors, etc. (**Figure 1**). Smart environment security systems can certainly play a role in keeping the home safe, but the basic packages offered by various manufacturers (Honeywell, Panasonic, Response, Samsung, and Yale) tend to contain rather limited technical protection, which does not provide sufficient security. security level for most real estate[2].

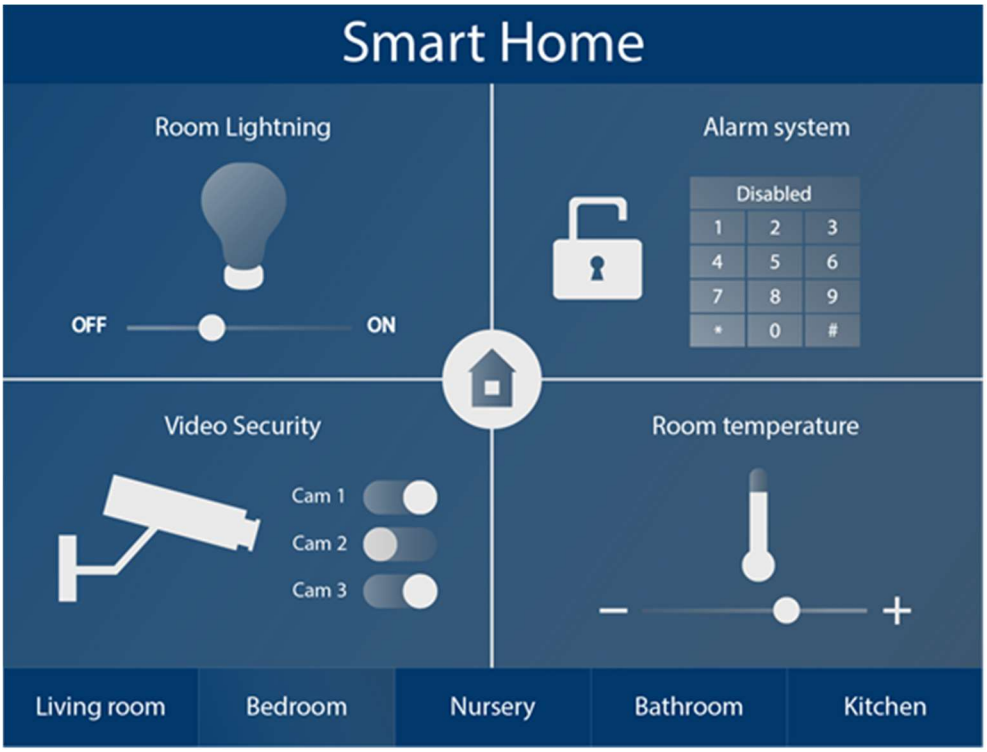


**Figure 1.** Smart environment security system option.

It should be noted that the most serious drawback among the systems offered on the market is the complete absence or very weak implementation of both built-in and plug-in SSS. This circumstance creates serious problems in the functioning of smart systems. Moreover, this directly applies to objects of various purposes and sizes—from a small apartment with a "smart home" to an enterprise or government institutions with installed SSS complexes. In addition, it is known that an increase in the number of connected devices and users to the smart environment inevitably leads to increased opportunities for cybercriminals to violate the IT security of the smart habitat infrastructure and the overall security of the facility[3].

The issue of ensuring the security of the smart environment is the issue of ensuring the safety of all aspects of life in modern society[4].

Solution—in the development of a system for the integrated management of heterogeneous safety and security systems (security and fire alarms, video surveillance, access control), innovative continuation—integration with the equipment of the "smart environment" based on each information technology space using artificial intelligence (AI) technologies and the Internet of Things (IoT).

To study this issue, it is necessary to consider the basic principles of building smart infrastructure, the risks and threats associated with its operation, as well as the place and role of technical security systems in the SH architecture.

## 2. Basic principles of construction and composition of smart infrastructure

The basic principle of constructing almost all smart systems is that all devices and systems in a house (facility) are connected to a single network, allowing them to interact with each other. In most projects, this is done using wired (Ethernet, USB, SPI, MIPI, I2C, RS-485, and others) and wireless (ZigBee, Bluetooth, Wi-Fi, NFC, RFID, LoRaWAN, SigFox NarrowBand-IoT, cellular network standards LTE, 5G (6G), satellite communications, etc.) communication methods[5–9]. In addition, the basic principles

that directly affect security include the choice of protocols for exchanging control signals and data, as well as the principle of unique IoT identification to enable integration.

In addition to the basic principles of building a smart infrastructure necessary for organizing SH protection, it is advisable to consider the typical infrastructure presented in **Figure 2**[4]:

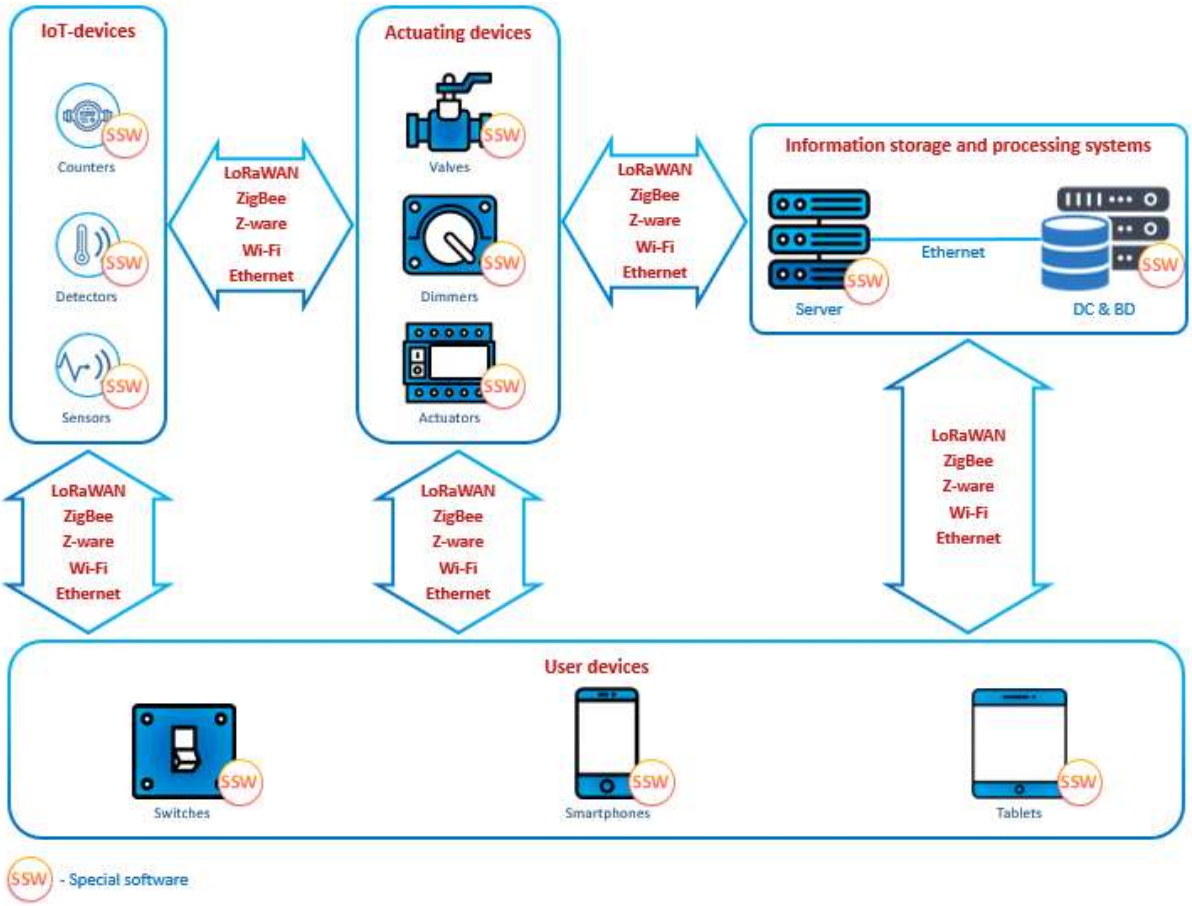


**Figure 2.** Typical smart environment infrastructure.

The smart environment infrastructure usually includes the following basic elements:

1) Sensors—various types of sensors for obtaining environmental parameters or monitoring user actions: smoke, lighting, motion sensors, video cameras, etc. (mainly IoT devices)[10].
2) Actuators—for controlling the load and activating terminal devices in the form of valves, relay drives, dimmers, and other actuators.
3) Information storage and processing systems—server equipment, DBMS, and other computing systems, the main purpose of which is to collect, process, and store data, as well as generate recommendations, reports, control actions, etc.
4) Information input and output (display) devices, interface devices—for reading user actions and displaying the status of the smart environment (switches, buttons, panels, smartphones, tablets, and other IoT devices)[11].
5) Communication means—means of receiving and transmitting data and protocols, the set of which varies widely depending on their purpose and resource limitations, as well as on the requirements of the use case. In addition, devices of this type should include switching, routing equipment, etc. (repeaters, switches, routers, etc.)[12].
6) Special software (SSW)—software designed for the operation of Smart Environment devices,

including. platforms and individual software modules (applications, libraries) responsible for data collection, device integration, real-time analytics, information visualization, data security, etc.[12].

The conducted study of the basic principles of construction and composition of the Smart Environment infrastructure clearly shows the need to modernize software and hardware related to the protection of confidentiality and integrity of information.

## 3. Security challenges for a smart environment

An analysis of existing options for organizing the security of SH infrastructures from the "smart home" to the "smart city" and industrial smart systems, as well as the development of cybercrime trends, showed that there are a number of significant gaps in their protection:

1) Failure of developers and installers to comply with security requirements at the stages of development, testing, and implementation of software and hardware for IoT devices and other elements of the smart environment.
2) The ever-expanding area of attacks on "smart things", as well as the constant improvement of the methods and speed of attacks by cybercriminals.
3) Failure to comply with security requirements when addressing issues of integration of various types of IoT devices.
4) The use of proprietary and little-known protocols that do not comply with international security standards, as well as the use of various methods of pairing devices through non-standard software and hardware connections, etc.
5) Lack of control over the periodic updating of SSW and IoT firmware (outdated software may not only contain errors and security holes but also have a high probability of already being hacked by cybercriminals).
6) Using 5G (6G) networks as a data transmission medium without taking into account the specific architecture and landscape of networks of these standards, which include a large number of connections and high throughput, functioning through cloud technology and using many different services, as well as placing equipment outside of protected areas contour.

According to a study by Kaspersky Lab JSC, in recent years there have been a number of high-profile cases of compromise of Internet of things devices by cybercriminals, namely[4]:

- 2016—Mirai botnet attack, when hundreds of thousands of compromised pluggable devices were involved in the botnet to perform malicious activities such as registration, emulation of "interested client" actions, password theft, and more. The Mirai botnet attack disrupted major services and websites such as Spotify, Netflix, and PayPal.
- 2018—VPNFilter malware infects about half a million routers in more than 50 countries, while VPNFilter malware can be installed on devices connected to the router and then, using malware, collect passing information, block network traffic, and steal passwords.
- 2020—Tesla Model X hack, when a cybersecurity expert hacked a Tesla Model X car in less than two minutes using a Bluetooth vulnerability, which, according to experts, applies to other car models using wireless access.
- 2021—Verkada video camera hack (Verkada is a surveillance camera company), when Swiss hackers gained access to 150,000 live feeds, including cameras at Tesla factories and warehouses, Cloudflare offices, Equinox gyms, hospitals, prisons, schools, police stations, and Verkada's own offices.
- 2022—the attack of the Zerobot botnet, which spreads through the exploitation of almost two dozen

vulnerabilities in IoT devices and various software (including F5 BIG-IP, Zyxel firewalls, Totolink and D-Link routers, and Hikvision cameras).

The above list of attacks by intruders on IoT (and this is a very small selective part) clearly demonstrates the seriousness of the possible consequences for all spheres of life in the modern world.

Thus, this is not only a matter of IT security; it is a matter of ensuring the security of all aspects of the life of modern society.

Based on the foregoing, we can conclude that it is necessary to carry out a rather extensive and labor-intensive set of measures, from monitoring suppliers of software and hardware to constant technical support at the stage of operation, modernization, expansion, etc. to ensure the required level of security of the smart environment[13].

To solve the problem, it is proposed to integrate into the technical security platform (hereinafter referred to as the specialized software platform, or SSP) already configured for a specific version of the smart environment object. In this case, it is advisable to first allocate into it the basic functionality of SSS, which takes into account the customer's unique requirements for protecting the object.

## 4. Features of implementation and innovative use of the integrated SSS platform

SSP is a universal platform integrated into the Smart Environment for the purpose of automated SSS management. SSP includes equipment (sensors and other IoT devices) of the following systems:

- fire alarm and evacuation and warning management;
- security alarm;
- monitoring to ensure dispatch processes (checking the availability of power and communications, liquid levels in containers and tanks, recording leaks, monitoring natural leaks and the presence of carbon monoxide, etc.).

The above systems, as a rule, include the following types of security and fire alarm sensors and monitoring of smart environment systems:

- motion sensor;
- presence sensor;
- leakage sensor;
- glass break sensor;
- opening sensor with shock and tilt sensor.
- supply voltage presence sensor;
- wall-mounted touch keyboard;
- internal (room) siren;
- external (street) siren;
- fire smoke detector;
- natural gas leak detector.
- multifunctional air quality sensor;
- magnetic contact sensors and others.

The innovativeness of the proposed approach to solving the security problems of the Smart Environment is as follows:

1) Creation of a universal SSW in the form of SSP that implements joint connection and use of

heterogeneous SSS types from different manufacturers. It should be noted that at the moment, when building security systems, there is no practice of developing a detailed plan for integrating information received from heterogeneous sources or SSS from different manufacturers, as well as the possibility of using it or transforming it for use within a smart environment (each system is closed, operates on their own, often morally "outdated", limited and unpromising standards, etc.). The proposed solution ensures the formation of a single universal approach to the SSS automation architecture system, which is implemented within the framework of the proposed SPP.

2) Bringing parameters of signals, protocols, interfaces, etc. to a single standard (through matching devices or "gatewaying"). heterogeneous SSS options when integrated within one system. To do this, at the first stage, an analysis of various IoT devices present in the smart environment is carried out for identification and categorization, which allows us to propose possible options for switching and transmitting information to centralized monitoring and security points (if necessary).

3) Application of modern principles of maintaining SSP security levels at the stage of connecting devices[14]. At the same time, special attention is paid to the organization of independent levels of IoT information exchange and SSS control devices, as well as security directly related to this process, including the organization of multi-level protection of promising 5G and 6G networks at the following three levels[15]:

The first level is protection at the level of implementation of technical solutions, construction of network infrastructure, and equipment placement options.

The second level is protection at the network infrastructure management level.

The third level is protection at the standard level.

4) Ensuring the protection of personal data. To reduce the likelihood of data de-anonymization in SSP, it is necessary to use new promising security methods, for example, the PSI3 algorithm, the hashing method, and also adding a dynamic random string for each element transmitted as part of information segments[16,17]. This allows you to significantly increase the hacking time and the amount of resources required by the attacker. In addition, the integrated use of the Diffie-Hellman algorithm and temporary keys increases the security of information exchange between software and hardware modules.

5) Use of a hybrid (domestic cloud and local) data storage system (DSS—data storage systems DSS) to maintain the functioning of SSP. It is worth noting that recently the customer has been urgently demanding the organization of storage of information circulating in SSS on a personal local resource ("on-premice" option), without excluding the possibility of using cloud DSS. In this regard, the proposed SSP solution provides for the organization of a combined method of storing information, in which it is possible not only to duplicate (back up) information but also to configure various options for its storage.

The proposed SSP or integrated SSS platform, implemented on the basis of the solutions proposed above, will provide the ability to implement full-featured management of heterogeneous SSS (security and fire alarms, video surveillance, access control, and other systems), as well as perform integration with Smart Environment equipment as part of a single information technology space with a multi-user interface based on IoT.

Summarizing the above, it can be noted that this will not only simplify the operating modes of the software and hardware of the SH infrastructure but also separate the functionality of the smart system and the technical security system.

## 5. Practical implementation

To study the proposed approach, a practical implementation of SSP was carried out. The following main software subsystems were included in the SSP infrastructure in the form of functional fragments of special software (SSW) (**Figure 3**):

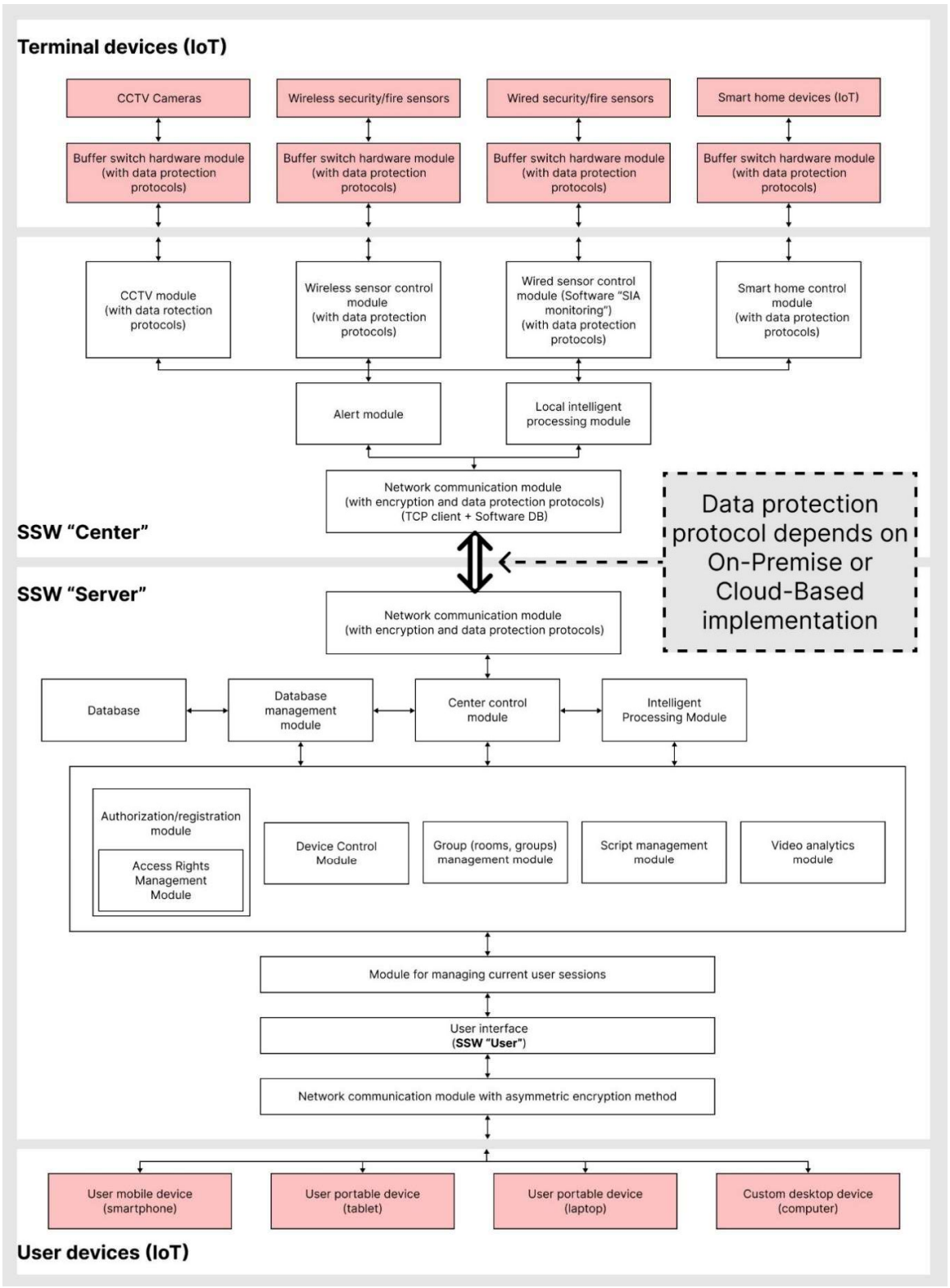


**Figure 3.** SSP block diagram.

1) SSW "server" ("BACK")—server software for collecting, analyzing (analytic), and other necessary processing of information. Software implementation tools (PSR) SSW—OS Ubuntu 20.04, programming language—Java 20 (OpenJDK 20), Java 17 (OpenJDK 17), main framework—Spring Boot, library for code reduction—Lombok, library for interaction with tokens—com. auth0.java-jwt, as well as other components—postgresql Driver, Jakarta. Mail.

Software modules of the open source software "server" (hereinafter referred to as the server):

- Network communication module.
- Encryption and decryption module.
- Center control module.
- OBD control module.
- Intelligent processing module.
- Video analytics module.
- Scenario management module.
- Grouping control module.
- Device control module.
- Authorization/registration module.

2) SSW "Center"—SSW interface with IoT and other terminal equipment (standard panels, control panels, etc.). PSR SSW—OS Ubuntu 20.04, programming language—C++, Qt 5.12.8.

Software modules of the open source software "center" (hereinafter referred to as the center):

- Wireless sensor control module.
- Wired sensor control module.
- Alert module.
- Local intellectual processing.
- Network interaction module.

When writing the center's software, modular programming is used. All modules are written in C++ using Qt libraries compiled from source code (only cross-platform free software is used). The center itself is focused on installation under the Linux system (at the customer's request, it can be installed on other operating systems).

3) SSW "user"—user interface SSW ("FRONT"), installed on IoT users. Software platform—node 20.3.1 with package manager—npm 9.6.7, web framework—Angular 15.2.6, reactive programming library—rxjs, programming language—typescript.

Graphical interface—organizes and manages user interaction with the system.

- The graphical interface is implemented both on mobile devices (OS—IOS, Android) and in the desktop version (OS—Windows, Linux). This feature allows the user to configure the security system himself, practically "from scratch," that is, add, remove devices, create scenarios, rooms, add new users, etc. The user can also adjust his security system at any time, for example, change sensor settings, scenarios, etc. Thus, to change the system settings (as well as for its initial configuration), it is not necessary to call an expensive specialist for these services.
- Network interaction module—works using the HTTPS protocol. Allows the exchange of messages between the user device and the server.

This equipment was connected directly to SSW "center" through a buffer switching hardware module

with specialized data protection protocols.

The SSP infrastructure contains specialized expansion points for deeper integration of SSS and smart systems based on the concepts of "smart enterprise", "smart office", "smart home", etc.

The presented SSP was integrated at the customer's facilities as part of two smart home configurations based on HDL and sibling equipment. Application of the proposed solution allowed:

1) Reduce by 20%–25% the use of expensive equipment from native smart system manufacturers.
2) Ensure the confidentiality of customer data.
3) Reduce by 18% the volume of data transmitted through the information channel of smart home equipment.
4) Organize the transmission of alarm information to the security company console, received from various sensors from various SSS sources from different manufacturers.

## 6. Conclusion

Rapidly developing smart environment technologies require constant attention to security issues. In this case, it is necessary to take into account the irreversibility of catastrophic consequences in the event of a violation of the protection of objects. Hacking IoT devices of smart homes, smart cities, and smart living environments will allow cybercriminals to control the living environment of people. In medicine and healthcare, in financial institutions (banks) and telephone companies, attackers' access to the smart systems used in these areas will lead to the disclosure and dissemination of personal (confidential) information about the patient, client, or subscriber. In addition, disruption of the functioning of medical devices, banking equipment, and telephone operator equipment leads not only to a deterioration in the quality of life but also to serious threats to its existence. Cyberattacks on industrial or military Internet of Things systems can lead to a number of irreversible destructive consequences[18].

The analysis of the SH infrastructure carried out by the authors clearly shows serious "gaps" in ensuring the security of facilities equipped with so-called smart systems.

In order to ensure the protection of such objects and the interests of users (customers), this work proposes an innovative technology that consists of the following stages:

1) Separation of the functionality of smart environment management systems and technical security systems.
2) Configuring specialized software in the form of SSP to service SSS.
3) Integration of SSP into the smart environment system.

The proposed solution provides the possibility of a single universal approach to the SSS automation architecture system, which is implemented within the framework of the proposed SSP and is ensured by:

- creation of a universal SSW in the form of SSP that implements the joint connection and use of heterogeneous SSS types from different manufacturers, bringing the parameters of signals, protocols, interfaces, etc. to a single standard. heterogeneous SSS variants;
- selection of optimal methods of switching and transmitting information to centralized monitoring and security points (if necessary), organizing independent levels of IoT information exchange and SSS control devices;
- organization of multi-level protection of promising networks of the 5G and 6G standard[18];
- ensuring the protection of personal data, reducing the likelihood of depersonalization;
- using a hybrid (cloud and local) data storage system, which allows not only to duplicate (back up) information, but also to configure various options for its storage.

It is necessary to emphasize the keen interest of the global technical community in solutions for combining and integrating various heterogeneous devices. This fact is evidenced by recent developments to create the "matter" standard. A group of companies such as Samsung, Xiaomi, Huawei, Google, Apple, and others are working on this problem. But so far, this is only a vision of the possibilities of combining software and devices without a finished product. At the same time, the proposed solution, after adaptation, certain settings, and subsequent modifications, will allow working with various technical security systems.

The proposed approach significantly increases the general and IT security of smart environment objects. It is also necessary to note the prospects for using this SPP for smart systems of large industrial facilities when building "smart cities" and various options for building SH.

## Author contributions

Conceptualization, GD and AD (Aleksandr Dik); methodology, GD; software, AD (Aleksandr Dik); validation, NS; formal analysis, AB; investigation, GD; resources, AD (Alexander Degtyarev); data curation, AB; writing—original draft preparation, GD; writing—review and editing, AD (Aleksandr Dik); visualization, NS; supervision, AB; project administration, GD; funding acquisition, AB. All authors have read and agreed to the published version of the manuscript.

## Conflict of interest

The authors declare no conflict of interest.

## References

1. Shipments of Smart Home Devices Fell in 2022, But a Return to Growth is Expected in 2023. Available online: https://www.idc.com/getdoc.jsp?containerId=prUS50541723 (accessed on 1 August 2023).
2. Smart home security system. Available online: https://in-bez.ru/articles/sistema-bezopasnosti-umnogo-doma/?ysclid=lrjooj1z9q866285954 (accessed on 1 October 2023).
3. Vereshchagina EA, Kapetsky IO, Yarmonov AS. 317 Security issues of the Internet of things. Available online: https://izd-mn.com/PDF/20MNNPU21.pdf (accessed on 10 January 2024).
4. Dik G, Bogdanov A, Shchegoleva N, et al. New Security Challenges of Internet of Things. In: Proceedings of the Computational Science and Its Applications—ICCSA 2023 Workshops; 3-6 July 2023; Athens, Greece. doi: 10.1007/978-3-031-37120-2_20
5. Roberto Sandre. Thread and ZigBee for home and building automation Systems Engineer.
6. Control Engineering Russia. Available online: https://controleng.ru/besprovodny-e-tehnologii/putivoditel-iot-3-wi-fi/ (accessed on 21 January 2024).
7. Bluetooth. Available online: https://www.bluetooth.com/learn-about-bluetooth/tech-overview (accessed on 21 January 2024).
8. Jonas Olsson. 6LoWPAN demystified. Texas Instruments. Available online: https://www.ti.com/lit/wp/swry013/swry013.pdf 510 (accessed on 21 January 2024).
9. Wltd. Available online: https://wltd.org/posts/thedifferences-between-z-wave-versions-made-easy (accessed on 21 January 2024).
10. Rayes A, Salam S. The Things in IoT: Sensors and Actuators//Internet of Things from Hype to Reality. Springer; 2017. pp. 57–77.
11. Lee P. Architecture of the Internet of Things. DMK Press; 2020.
12. Basic protocols, message sequence charts, and the verification of requirements specifications. Computer Networks. 2005; 49(5): 661-675.
13. Chantsis F, Stais I, Calderon P, Deirmenzoglu E. Woods B. Practical Hacking of the Internet of Things. DMK Press; 2022.
14. Leonova EM. About the problem of interfacing technical notification means of different manufacturers. Current Issues of Natural Science. 2022; 699-704.
15. Bogdanov A, Shchegoleva N, Dik G, et al. "Smart Habitat": Features of Building It Infrastructure, Main Problems of Building Data Networks Using 5G (6G) Technologies. In: Proceedings of the Computational

Science and Its Applications—ICCSA 2022 Workshops; 4-7 July 2022; Malaga, Spain. pp. 628-638. doi: 10.1007/978-3-031-10542-5_43

16. Bogdanov A, Dik A, Dik G, et al. K-Anonymity Versus PSI3 for Depersonalization and Security Assessment of Large Data Structures. International Conference on Computational Science and Its Applications. Springer Nature Switzerland; 2023. pp. 317-333.
17. Bogdanov AV, Dik A, Shchegoleva N, et al. Protection of personal data using anonymization. In: Proceedings of the Computational Science and Its Applications—ICCSA 2021: 21st International Conference; 13-16 September 2021; Cagliari, Italy. pp. 447-459.
18. Dik G, Bogdanov A, Shchegoleva N, et al. Challenges of IoT Identification and Multi-Level Protection in Integrated Data Transmission Networks Based on 5G/6G Technologies. Computers. 2022; 11(12): 178. doi: 10.3390/computers11120178