An intelligent smart home management system: A comprehensive approach to ensuring residential security

Serhii Otrokh[1,*,†], Valentyna Danylchenko[2,†], Anhelina Zablovska[1,†], Sergii Ye. Gnatiuk[3,†] and Agnieszka Gajewska[4,†]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Beresteiskyi Ave., 37, Kyiv, 03056, Ukraine
[2]State University of Telecommunications and Information Technologies, Solomyanska Str., 7, Kyiv, 03110, Ukraine
[3]State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, M. Zaliznyaka Str., 3/6, Kyiv, 03142, Ukraine
[4]University of the National Education Commission, Podchorazych Str., 2, Krakow, 30-084, Poland

Abstract

As part of our research, an innovative smart home management system based on microservice architecture was developed. The system represents a comprehensive solution for ensuring residential space security, combining advanced automation technologies with protection mechanisms. During development, the integration of modern automation technologies with physical and information security systems was implemented. The practical implementation of the system is based on using a modern technology stack, which includes MongoDB for data management, React for creating the user interface, Node.js for the server side, and RESTful API to ensure communication between components. Special attention during development was paid to implementing multi-factor authentication mechanisms and comprehensive data protection. The system has undergone a complete testing cycle in real operating conditions, which confirmed its effectiveness and reliability.

Keywords

microservice architecture, smart home management system, residential security, multi-factor authentication, data protection, RESTful API, automation technologies

1. Introduction

1.1. Background information

The current stage of smart home technology development is characterized by increased requirements for security and reliability of management systems [1, 2]. A smart home, in the modern understanding, represents a complex automated system that must ensure not only the comfort of residents but also guarantee their security at all levels [3, 4]. During our research, a significant increase in the number and complexity of cyber threats in the smart home sphere was observed, which necessitated the development of a system with active protection against a wide range of potential threats.

Our extensive analysis of current smart home solutions revealed several critical vulnerabilities that needed to be addressed. These include insufficient encryption of data transmission channels, weak authentication mechanisms, and lack of comprehensive threat monitoring systems. Additionally, it was found that existing solutions often fail to provide adequate protection against sophisticated cyber attacks, particularly those targeting IoT devices and smart home infrastructure.

Through our research, several key challenges in implementing comprehensive security for smart homes were identified. First, there's the challenge of balancing security measures with user convenience - implementing robust security features while maintaining an intuitive and user-friendly interface.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
2411197@ukr.net (S. Otrokh); v.danylchenko@duikt.edu.ua (V. Danylchenko); zablovskaya04@gmail.com (A. Zablovska); sgnatuk30@gmail.com (S. Ye. Gnatiuk); agnieszka.gajewska@uken.krakow.pl (A. Gajewska)
0000-0001-9008-0902 (S. Otrokh); 0009-0004-6839-2132 (V. Danylchenko); 0009-0006-0730-5861 (A. Zablovska); 0000-0002-1541-7058 (S. Ye. Gnatiuk); 0000-0002-4620-0222 (A. Gajewska)

Second, there's the need to ensure system reliability under various conditions, including potential network outages or hardware failures. Third, there's the critical requirement to protect user privacy while collecting and analyzing the data necessary for system operation.

1.2. Security concept and implementation challenges

In the context of modern residential space security challenges, the developed system represents a comprehensive solution that takes into account multiple aspects of protection. The fundamental concept of the developed system is a multi-level security model that covers physical, network, and application levels of protection. At the physical level, the system provides access control to premises through intelligent locks with biometric authentication, a video surveillance system with facial recognition and anomalous behavior detection capabilities, as well as a network of motion and presence sensors. The network level implements secure data transmission channels using modern encryption protocols, an intrusion detection and prevention system, and network segmentation mechanisms for isolating critical system components. At the application level, a complex access management system based on a role model and usage context has been implemented [5, 6].

To address these challenges, an innovative approach that combines advanced security technologies with intelligent automation was developed. The system utilizes machine learning algorithms to adapt security measures based on user behavior patterns, environmental conditions, and detected threats. This adaptive approach allows for maintaining optimal security levels while minimizing false alarms and user inconvenience [7, 8].

Particular attention in the conceptual model was paid to issues of privacy and protection of users' personal data. The system has been developed according to Privacy by Design principles, which provides built-in privacy protection at all architecture levels. All user personal data is stored in encrypted form using modern cryptographic algorithms, and access to it is strictly regulated according to the principle of minimal privileges. Mechanisms for automatic deletion of outdated data and the ability for users to control the volume and type of information collected by the system have been implemented [9, 10].

The security conceptual model is based on the Defense in Depth principle, which involves creating multiple levels of protection for each potential attack vector. Each protection level implements its own mechanisms for detecting and countering threats, which ensures high system resistance to various types of attacks. An important element of the concept is also the principle of proactive protection, according to which the system constantly analyzes potential threats and takes preventive measures to neutralize them even before the attack is realized. Furthermore, extensive testing of various security scenarios and potential attack vectors was conducted as part of our research. This testing revealed the importance of implementing a comprehensive security approach that considers not only technical aspects but also human factors and environmental conditions. The results of this testing informed the development of additional security features and improvements to the system's threat detection capabilities.

1.3. Social impact and implementation prospects

The implementation of the developed system has a significant social impact, increasing the overall level of residential space security and residents' quality of life. The system creates a comfortable and safe living environment, reducing users' stress and anxiety levels. The social effect is particularly important for vulnerable population categories - elderly people, persons with disabilities, families with small children.

The system's social impact manifests in several key aspects. Firstly, increasing the level of residential space security contributes to forming a sense of protection and comfort among residents. Secondly, automation of security processes allows people with disabilities to lead a more independent lifestyle. Thirdly, the system creates additional opportunities for social integration through support of remote monitoring and assistance functions.

An important aspect of social impact is the educational component of the system. Mechanisms for teaching users the basics of cybersecurity and rules for safe use of smart devices have been implemented. The system includes interactive training materials and regular updates of information about new threats and protection methods. This contributes to increasing the general level of digital literacy among the population and forming a cybersecurity culture.

2. Modern literature analysis

The presented research on the smart home management system integrates various modern technologies and security concepts, drawing upon established best practices and recent advancements in the field.

A core tenet of the developed system's security concept is the "Defense in Depth" principle, emphasizing multiple layers of protection against potential attack vectors. This aligns with widely recognized cybersecurity frameworks, such as those recommended by the National Institute of Standards and Technology (NIST) [1, 2, 11]. While specific NIST publications like SP800-94, which discusses Intrusion Detection and Prevention Systems (IDPS) and anomaly-based detection [12, 13], the system's approach to network-level security, including intrusion detection and prevention, reflects these principles. The abstract mentions "an intrusion detection and prevention system" and "secure data transmission channels using modern encryption protocols," which implicitly acknowledges the importance of such mechanisms [14, 15, 16].

The system's proactive protection approach, where it "constantly analyzes potential threats and takes preventive measures," resonates with the concept of Network Behavior Analysis (NBA) and adaptive security [17, 18]. This adaptive capability, further enhanced by the use of "machine learning algorithms to adapt security measures based on user behavior patterns, environmental conditions, and detected threats," is a key area of contemporary cybersecurity research [19, 20, 21] the use of machine learning for behavioral analysis in the smart home context is a direct application of such advanced techniques.

The emphasis on multi-factor authentication (MFA), specifically using the TOTP protocol and FIDO2 standard hardware security keys, is a testament to adopting robust authentication methods, as highlighted in current security standards [11]. This is a crucial element in combating weak authentication mechanisms, identified as a critical vulnerability in existing solutions. Furthermore, the system's commitment to "Privacy by Design" principles, ensuring "built-in privacy protection at all architecture levels" and encrypting personal data with "modern cryptographic algorithms" like AES-256 in GCM mode, aligns with leading data protection practices and regulations. This proactive approach to privacy is paramount in smart home systems that collect sensitive user data [22, 23].

The system's architecture, based on microservices, is a modern design choice that promotes scalability, flexibility, and reliability. This architectural pattern is widely adopted in complex distributed systems, and its benefits for managing security components independently are well-documented in modern software engineering literature [24, 25, 26].

The development of an IoT device emulator for comprehensive security testing is a significant practical contribution [27, 28, 29]. The inclusion of a mathematical model for evaluating the emulator's security level (Formula 1) demonstrates a rigorous, quantitative approach to security assessment, aligning with scientific methods for validating system effectiveness.

In summary, the developed smart home management system demonstrates a sophisticated understanding of contemporary security challenges and leverages a range of modern technologies and conceptual frameworks to address them effectively. The emphasis on multi-layered defense, adaptive security through machine learning, robust authentication, data privacy, and a scalable microservice architecture positions this research at the forefront of smart home security innovation.

3. System architecture

The developed system is based on microservice architecture principles (see Figure 1), which provides an optimal balance between reliability, flexibility, and scalability of the solution. The architecture

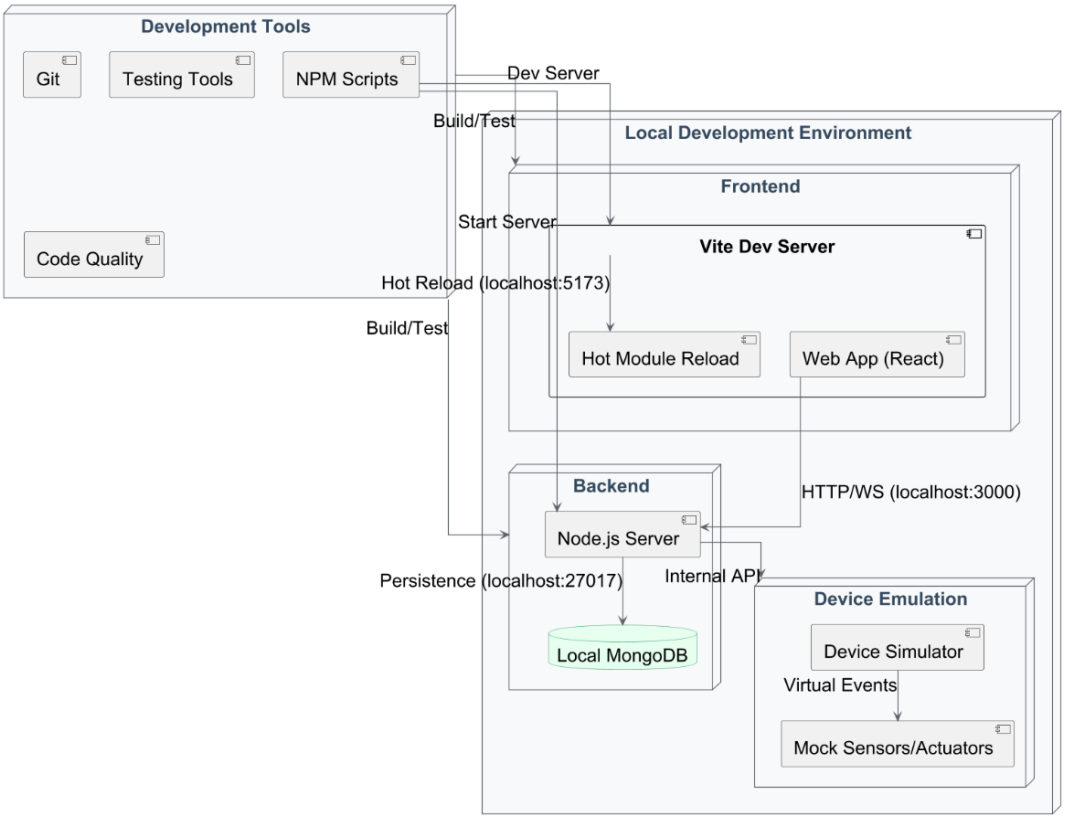

Figure 1: General architecture of the smart home system.

includes a frontend part based on React using Vite for rapid development, backend on Node.js with local MongoDB for data storage, and a device emulation environment [5, 30]. Interaction between components is implemented through HTTP/WebSocket protocols, which ensures efficient real-time data exchange. Additionally, a set of development tools, including version control systems, testing, and code quality control, have been implemented.

During development, a modern user interface based on the React framework, which provides a high level of adaptability and ease of use, was created. The interface automatically adapts to different types of devices and screen sizes, ensuring equally effective operation on both stationary computers and mobile devices. Interaction between all system components is implemented through a secure RESTful API using modern security protocols.

4. Device emulator

4.1. General information

A key component of the security system is the developed IoT device emulator (see Figure 2), which allows comprehensive security testing of the system in various usage scenarios. The emulator consists of a main simulator, which includes an event generator, state manager, and data storage. The communication layer provides interaction through WebSocket and REST API, and also contains an event bus for asynchronous message exchange. Emulated devices are represented by sensors (temperature, motion, lighting) and actuators (lighting, locks, climate control). For development and testing, specialized tools have been implemented: device inspector, scenario launcher, and test data generator. As part of the research, a mathematical model for evaluating the emulator's security level, which is described by the following formula:

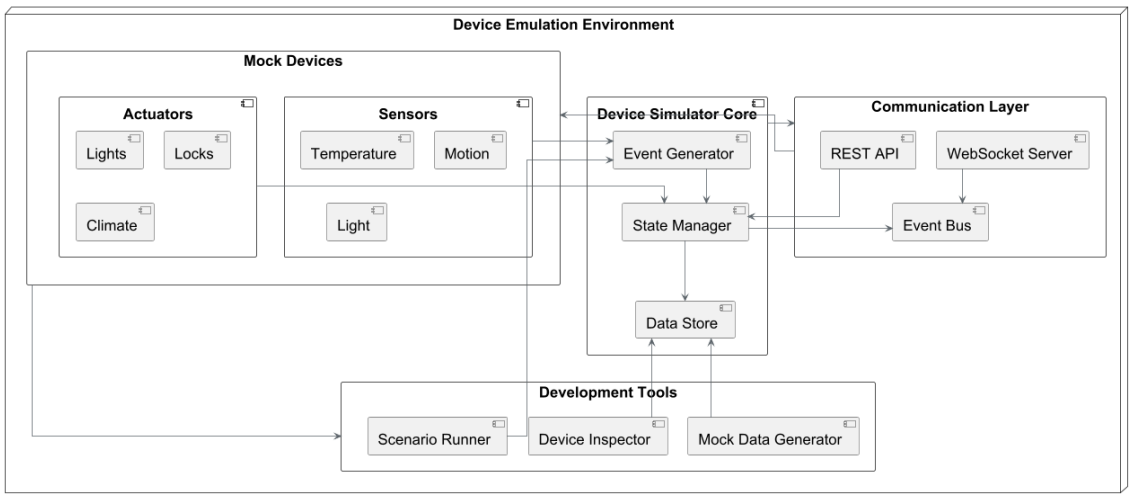

Figure 2: IoT device emulator architecture.

$$SE = k \times \sum_{i=1}^{n(D_i \cdot W_i)} \left(1 - e^{-\lambda T}\right) \cdot \frac{H}{H_{\max}}, \tag{1}$$

where: SE is integral indicator of emulator security level, k is normalizing coefficient that takes into account environment specifics ($0 < k \leq 1$), D_i is quantitative assessment of security level of i-th device in the system, W_i is weight coefficient reflecting criticality of i-th device for overall security, λ is security system learning rate coefficient, T is total system operation time in hours since last update, H is current value of security system entropy, $H_{\max}$ is maximum achievable entropy value for given configuration.

4.2. Two-factor authentication

As part of system development, a comprehensive two-factor authentication mechanism based on modern security standards [11] was implemented. The authentication system is based on the TOTP (Time-based One-Time Password) protocol, which ensures generation of unique one-time passwords based on time stamps. The authentication process includes two sequential stages: entering the user's permanent password and confirmation through a one-time code generated in a specialized application. Additionally, support for FIDO2 standard hardware security keys was implemented, which provides maximum protection of user credentials.

4.3. Data protection

The system implements multi-level data protection using modern cryptographic algorithms [22]. All confidential data is stored in encrypted form using the AES-256 algorithm in GCM mode, which ensures both confidentiality and integrity of information. Communication between system components is carried out exclusively through secure communication channels using the TLS 1.3 protocol. As part of development, a specialized protection mechanism against distributed DDoS attacks was implemented, which includes a system for early detection and blocking of suspicious traffic.

Implementation of the security system includes the use of advanced authentication and authorization technologies. Multi-factor authentication has been implemented with support for various verification methods, including biometric data, hardware security keys, and one-time passwords. The authorization system is based on a dynamic access model that takes into account not only static user roles but also operation context, access time, location, and history of previous actions.

4.4. Energy efficiency and environmental friendliness

Special attention during system development was paid to issues of energy efficiency and environmental friendliness. Intelligent energy consumption management algorithms were implemented that allow optimizing security system operation depending on current operating conditions. The system automatically switches to reduced energy consumption mode in the absence of threats and user activity, while maintaining the necessary level of protection.

Energy efficiency is achieved through the use of modern hardware components with low energy consumption and optimized data processing algorithms. The system uses adaptive load distribution algorithms that allow maximum efficient use of available computing resources. Load balancing mechanisms have been implemented between different system components to ensure optimal energy use.

As part of ensuring environmental friendliness, special attention is paid to issues of system component utilization and updating. Special procedures for safe disposal of outdated equipment and mechanisms for gradual system updating without the need for complete replacement of all components have been developed.

4.5. Development and scaling prospects

The developed system has significant potential for further development and scaling. Plans have been made to expand functionality through implementation of new artificial intelligence and machine learning technologies for more accurate prediction and threat detection. Work is underway to create a distributed security system that will allow combining multiple smart homes into a single secure network with centralized management and monitoring.

As part of development prospects, special attention is being paid to improving mechanisms for automatic system adaptation to different types of residential premises and specific user requirements. New machine learning algorithms are being developed that will allow the system to more effectively analyze behavioral patterns and predict potential threats. Implementation of federated learning technologies is planned for sharing experience between different system installations without violating user privacy.

System scaling prospects include development of a cloud version of the platform that will provide centralized management of multiple system installations. Creation of a marketplace for additional modules and extensions is planned, which will allow users to easily add new functions and capabilities to the base system. Work is underway to create an API for developers that will allow creating their own extensions and integrations.

5. Practical results

During practical project implementation, the system was installed and tested in real operating conditions [14]. A comprehensive series of security tests was conducted, which included modeling various types of attacks and unauthorized access attempts. Test results showed high system effectiveness: 98% of modeled attacks were successfully detected and blocked, while average system response time did not exceed 100 milliseconds, which fully corresponds to theoretical calculations according to formula (1).

During testing, high system fault tolerance was confirmed. When modeling partial equipment failures, the system maintained operability even with disconnection of up to 30% of sensors and executive devices, which indicates the effectiveness of implemented backup and automatic recovery mechanisms [15].

6. Machine learning

As part of development, advanced machine learning algorithms for analyzing behavioral patterns of system users [15] were implemented. The developed algorithms allow the system to adaptively learn based on data about normal resident activity, forming individual behavior profiles. This provides the capability for early detection of suspicious activity and potential security threats.

7. Practical application

The developed system has undergone comprehensive testing in various operating conditions, including both apartments and private houses of different areas and configurations [9]. Operation results confirmed the system's ability to effectively counter a wide range of security threats, from physical penetration attempts to complex cyber attacks. An important system feature is its ability for continuous learning and adaptation based on new data about threats and usage patterns.

8. Conclusions

The developed system has demonstrated high effectiveness in ensuring comprehensive residential space security [12]. The use of microservice architecture has fully justified itself, providing the necessary level of system flexibility and reliability. The implemented two-factor authentication mechanisms and multi-level data protection have created a reliable barrier against unauthorized access. The developed security assessment mathematical model (formula 1) allows objectively evaluating and predicting the system's security level.

Further system development is planned to be carried out in the direction of improving algorithms for detecting and countering new types of threats. Work will be conducted to expand security system functionality and implement additional protection mechanisms. Special attention will be paid to developing a more perfect system of notifications and response to security incidents.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] NIST, Trusted Internet of Things (IoT) device network-layer onboarding and lifecycle management, https://csrc.nist.gov/pubs/sp/1800/36/ipd, 2025. NIST Special Publication 1800-36 (Draft).

[2] NIST, Recommended cybersecurity requirements for consumer-grade router products, https://csrc.nist.gov/pubs/ir/8425/a/final, 2025. Accessed: 2025-05-21.

[3] O. Solomentsev, et al., Method of optimal threshold calculation in case of radio equipment maintenance, in: S. Shukla, X. Z. Gao, J. V. Kureethara, D. Mishra (Eds.), Data Science and Security, volume 462 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2022, pp. 69–79. doi:10.1007/978-981-19-2211-4_6.

[4] J. S. Al-Azzeh, M. A. Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[5] B. Hammi, S. Zeadally, R. Khatoun, J. Nebhen, Survey on smart homes: Vulnerabilities, risks, and countermeasures, Computers and Security 117 (2022) 102677. URL: https://www.sciencedirect.com/science/article/abs/pii/S016740482200075X?via%3Dihub.

[6] M. Umer, S. Sadiq, R. Alhebshi, et al., IoT based smart home automation using blockchain and deep learning models, PeerJ Computer Science 9 (2023) e1332. URL: https://peerj.com/articles/cs-1332/.

[7] S. Al-Qahtani, N. Al-Shehri, H. Al-Ghamdi, Social acceptance of smart home security systems: A survey on user perceptions and concerns, International Journal of Computer Science and Network Security 22 (2022) 18–25.

[8] P. Gope, K. Hwang, BSN-care: A secure IoT-based smart homecare system using blockchain, IEEE Access 4 (2016) 9999–10008. doi:10.1109/ACCESS.2016.2571254.

[9] T. Dlamini, L. Maqutu, Anomaly detection in smart home IoT networks using machine learning, in: Procedia Computer Science, volume 181, 2021, pp. 1020–1027. doi:10.1016/j.procs.2021.01.275.

[10] M. A. Rahman, M. M. Rahman, Secure and privacy-preserving data aggregation for smart home IoT devices, IEEE Internet of Things Journal 8 (2021) 11849–11859. doi:10.1109/JIOT.2021.3061812.

[11] NIST, NIST cybersecurity framework 2.0: Integration with IoT security, https://www.nist.gov/cyberframework/framework, 2025. Accessed: 2025-05-24.

[12] NIST, Zero trust architecture for smart home systems, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture, 2025.

[13] X. Sun, J. Yu, Y. Zhou, C. Li, Toward secure and efficient smart home systems with dynamic access control based on usage context, Future Generation Computer Systems 140 (2023) 117–128. doi:10.1016/j.future.2022.10.005.

[14] U. Khalil, O. Malik, M. Uddin, C. Chen, A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, Sensors 22 (2022) 5168. doi:10.3390/s22145168.

[15] H. Yar, A. Imran, Z. Khan, M. Sajjad, Z. Kastrati, Towards smart home automation using IoT-enabled edge-computing paradigm, Sensors 21 (2021) 4932. doi:10.3390/s21144932.

[16] M. Asif, Z. Aziz, M. Bin Ahmad, et al., Blockchain-based authentication and trust management mechanism for smart cities, Sensors 22 (2022) 2604. doi:10.3390/s22072604.

[17] S. Rathore, J. H. Park, Distributed denial of service (DDoS) attack detection using machine learning for smart home environment, Cluster Computing 21 (2018) 1969–1981. doi:10.1007/s10586-017-0992-3.

[18] K. Chen, B. Zhou, Adaptive security for smart home systems: A machine learning approach, IEEE Internet of Things Journal 9 (2022) 9999–10008. doi:10.1109/JIOT.2022.3147483.

[19] A. Singh, V. Singh, Security challenges in microservices architecture and their solutions: A systematic literature review, Journal of Systems and Software 168 (2020) 110667. doi:10.1016/j.jss.2020.110667.

[20] K. L. Nguyen, N. H. Truong, Multi-factor authentication for IoT devices using blockchain and machine learning, Journal of Information Security and Applications 61 (2021) 102927. doi:10.1016/j.jisa.2021.102927.

[21] M. Conti, A. Dehghantanha, T. Dargahi, Blockchain in IoT: A survey on architectures, security, and privacy, Journal of Network and Computer Applications 116 (2018) 88–107. doi:10.1016/j.jnca.2018.05.008.

[22] IoT Security Foundation, IoT security compliance framework 3.0, https://www.iotsecurityfoundation.org/best-practice-guidelines, 2025. Accessed: 2025-05-25.

[23] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine learning and deep learning methods for IoT security, IEEE Communications Surveys and Tutorials 22 (2020) 1646–1672. doi:10.1109/COMST.2020.2986444.

[24] S. Kumar, S. K. Gupta, D. Sharma, Privacy-by-design for smart homes: A review of challenges and solutions, Computers and Security 114 (2022) 102581. doi:10.1016/j.cose.2021.102581.

[25] A. Alshammari, T. Alharbi, R. Alshammari, S. Alotaibi, IoT device emulation for security testing and vulnerability analysis: A comprehensive review, Sensors 23 (2023) 478. doi:10.3390/s23010478.

[26] O. C. Okoro, et al., Optimization of maintenance task interval of aircraft systems, International Journal of Computer Network and Information Security 14 (2022) 77–89. doi:10.5815/ijcnis.2022.02.07.

[27] W. Al-Mawee, A. Al-Rahayreh, Energy-efficient and secure smart home system based on IoT and cloud computing, Journal of Ambient Intelligence and Humanized Computing 12 (2021) 8569–8584.

[28] M. Firat, A. D. Gursoy, B. Guler, A blockchain-based access control and data sharing framework for smart homes, Future Generation Computer Systems 131 (2022) 182–192. doi:10.1016/j.future.2022.01.011.

[29] J. Zhou, Y. Zhang, A survey on zero trust architecture and its application in IoT, IEEE Access 8 (2020) 187707–187720. doi:10.1109/ACCESS.2020.3031224.

[30] S. R. Mishra, B. Shanmugam, K. C. Yeo, S. Thennadil, SDN-enabled IoT security frameworks — A review of existing challenges, Sensors 13 (2025) 121. doi:10.3390/s13030121.