# Advancing Network Security in Smart Homes: Intrusion Prevention Technologies in IoT Systems

Ruijie Yin

School of Electrical Engineering, Sichuan University, Chengdu, China

2021141440497@stu.scu.edu.cn

**Abstract.** Smart home systems, increasingly integrated with Internet of Things (IoT) technology, are transforming residential environments by enhancing convenience and energy efficiency. However, this integration expands the attack surface, presenting substantial security challenges. The proliferation of connected devices in smart homes increases the risk of unauthorized access and personal data breaches. This paper aims to provide a comprehensive analysis of the security vulnerabilities associated with smart home systems. It will evaluate existing protective measures and the effectiveness of these systems against contemporary network intrusion techniques. By exploring potential weaknesses in device security, network protocols, and user interfaces, this study will propose enhanced strategies for safeguarding user data and ensuring system integrity in the IoT ecosystem. The goal is to develop a set of robust security protocols that can be adopted by industry stakeholders to mitigate risks and protect user privacy in the evolving landscape of smart home technologies. This analysis is crucial for understanding the trade-offs between convenience and security in connected home environments.

**Keywords:** IoT internet, security network, intrusion detection technology.

## 1. Introduction

The burgeoning smart home market is a testament to the expansive potential and growth within this sector. Research by IHS Markit highlights the pivotal role of IoT devices across various applications, underscoring their dominance in the smart home domain. As illustrated in Figure 1, the smart home category leads with a staggering 8.226 billion IoT devices installed, significantly outpacing other sectors. This data not only reflects the current scale of IoT integration into home automation but also underscores the increasing reliance on these technologies to enhance residential environments and user experiences.

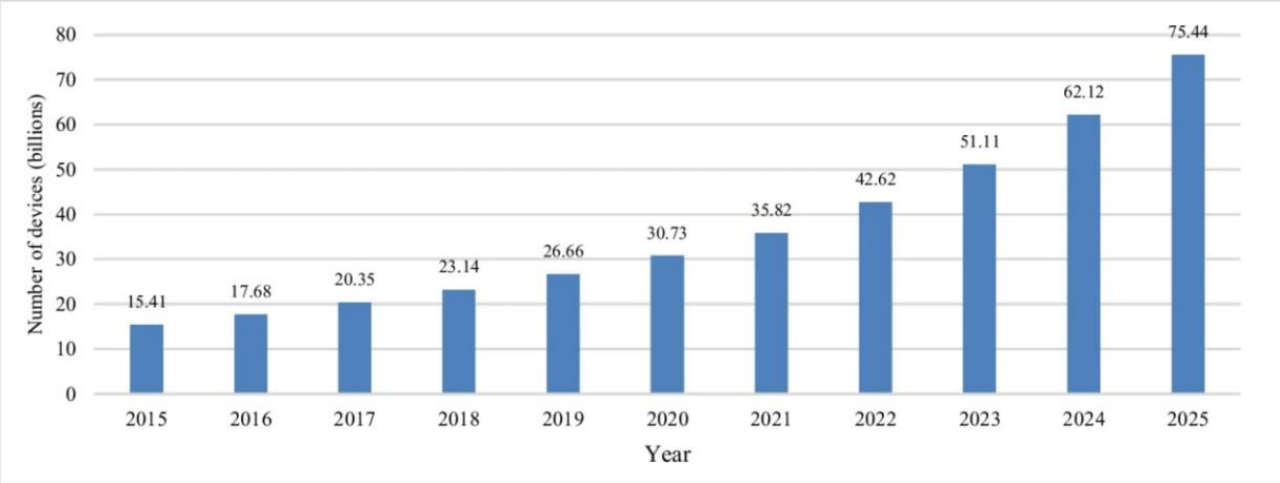


**Fig. 1** Estimate of the total number of Internet of Things devices worldwide by 2025 [1].

Such huge data illustrates that the range of applications for IoT devices is gradually expanding. Next, focusing the data on the element of smart home, Figure 2 determines the trend of smart home in the IoT field by the growth rate of.

One of the main concerns with IoT is security., about which summarise three reasons: Initially, an uncontrollable. When sensors, actuators, or other linked devices are utilized maliciously, IoT systems not only compromise users' privacy but also result in physical injury. Second, they point to the risks faced by manufacturers. If an attacker obtains access to sensitive information or proprietary assets through an IOT system, valuable information and reputation may be lost. Third, due to the highly interconnected nature of IoT systems, the impact of an attack is not limited to specific devices or networks. In this sense, the saying "the strength of a chain depends on its weakest link" is very applicable; the security of an IoT network depends on its weakest device [2]. In this paper, the current research on smart home security is divided into three major aspects: platform security, device security and communication security. Device security is the security concern directly related to smart home terminal devices; platform security is the security concern related to network communication; and communication security is the security concern related to the different security issues present in the platform design and implementation of smart home platform vendors. In Table 1, the research problems in each aspect are listed, and this classification is used as a theme to introduce the security problems of smart home system and research status [3].

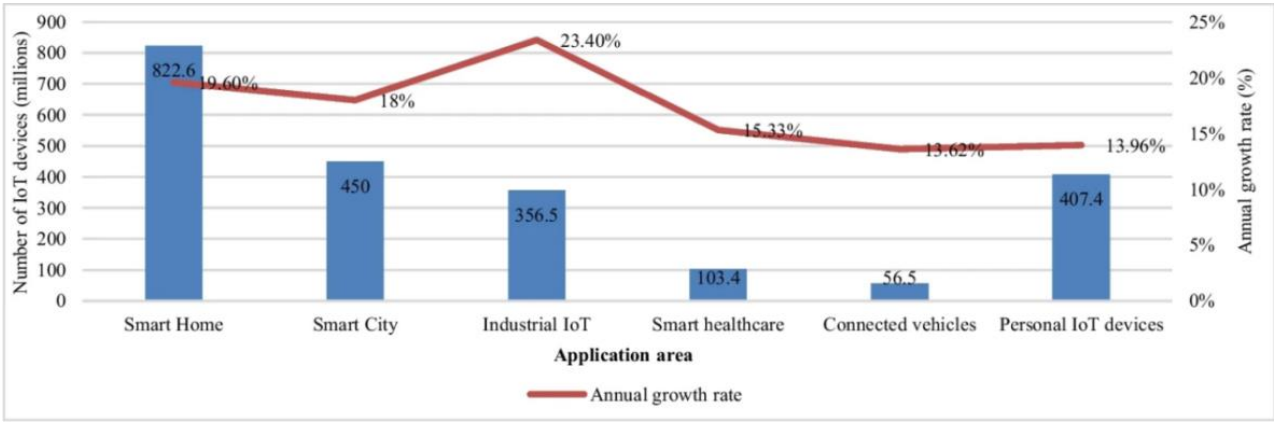


**Fig. 2** The quantity and yearly growth rate of IoT devices according to application [2].

**Table 1.** Smart Home Security Research Issues [4].

| Categories | Research Issues |
|---|---|
| Platform Security | Authentication for the smart home |
| | Access control for the smart home |
| | Trigger-Action security |
| Device Security | Security and privacy of the smart speaker |
| | Vulnerability discovery in the smart home device |
| | Side channel attack in the smart home device |
| Communication Security | Vulnerability discovery in the communication protocol |
| | Network traffic analysis for the smart home |

In fact, the smart home is closely connected to the platform, the information transmission process and the platform itself are at risk of intrusion. Especially the authentication mechanism of identity recognition, there are already a large number of invasion means that can bypass the authentication and directly invade the device. In light of the context of this investigation, this research aims to analyze the newly implemented defenses against intrusions.

# 2. Related Research on Network Intrusion

## 2.1. Protections in the IoT Field

### 2.1.1. Conventional protection IoT protection strategies

This paper will present some security countermeasures for IoT with respect to specific IoT functions and security goals.

Based on the enumeration of for this element, it will first be analysed by means of an authentication measure [5]. This is a scheme proposed by Zhao et al. for mutual authentication of IoT platforms and terminals [6]. The combination of hash functions with feature extraction is the foundation of this technique, but the shortcoming is that most of the implementation of this method is still in the theoretical stage, and there are relatively few practical applications. In, another method of using authentication in Internet sensor nodes is mentioned - the request-response mechanism of one-time password mechanism [7]. This technique works with a wide range of Internet-connected devices and is more adaptable, while at the same time making the security protection no longer remain at the theoretical level for the time being.

Another dimension of the approach mentioned in is the creation of trust. As IoT devices may be physically moved from one owner to another, trust must be built between the two owners to enable a seamless movement of rights and access control for IoT technology. This approach requires the creation of keys and tokens, and therefore requires to some extent the support of the manufacturer.

### 2.1.2. Mechanisms of IPS operation

An Intrusion Prevention System (IPS), also known as an IDPS, is an organised security framework for monitoring network organisations and formulating frameworks for malicious behaviour. An intrusion prevention system's primary functions include detecting harmful activity, recording information about it, trying to thwart it, and reporting it. The passage aims to develop host-based intrusion prevention systems (IPS) that can fend against host-side network intrusion threats. Creating a lightweight intrusion prevention software for Ubuntu Linux OS systems with an administration console, adding network monitoring capabilities, developing statistical and signature-based security features for early cyber-attack detection, putting in place a response mechanism for cyber-attacks, and offering a mechanism to prevent cyber-attacks are all the objectives of the host-based intrusion prevention system. It establishes a reaction mechanism against cyberattacks, adds statistical and signature-based security measures for early cyberattack detection, and allows customers to easily create their own cyber-security policies and utilize the IPS software to enforce them [8].

The previous defence system NIDS is divided into hybrid mode and network mode, this mode has a relatively big defect, that is, only to mark-based attacks to make identification judgments and responses, and for the intrusion of unfamiliar signals, this protection mode is very easy to appear difficult to cope with the problem of leading to system damage. But relatively, IPS in this field to deal with this problem more funny, because it can be identified through the event and known vulnerabilities to compare once to achieve the detection of the location of the threat (this process is also often referred to as the identification of the IPS). Botnets, for instance, use personally identifiable information (PII) to target DoS assaults. One sign of a deadly assault may be an atypically big ping packet.

However, due to the emergence of too many new types of attacks, the IPS criteria for unknown signals need to be updated all the time. This requires IPS administrators to always specify new rules for identifying intrusion signals, and even to identify intrusion signals and understand their operating mechanisms to avoid duplicate localisation. This process causes great inconvenience. Therefore, the leading manufacturers of IPSs apply a new system of rules to identify intrusion signals - validity identification: determining whether an entity is a foreign unit by identifying whether it plays a valid role in the system. While this rule needs to be tightly formulated to prevent the removal of units from the system itself, the completed rule is more convenient and allows for the identification of intruding units based on different locations. Similar rules exist for anomaly-based detection, where any new

activity that a newly added signal is involved in is considered new, and similar conclusions can be reached by determining whether the new activity is valuable or not.

### 2.2. Advanced network intrusion towards IoT system

Attacks against the IoT can come from many sources, and it is well known that the IoT consists of multiple parts: layer three: application, network, and physical. Each of them may have vulnerabilities and different aspects of attack threats. A concrete demonstration is shown in Figure 3:

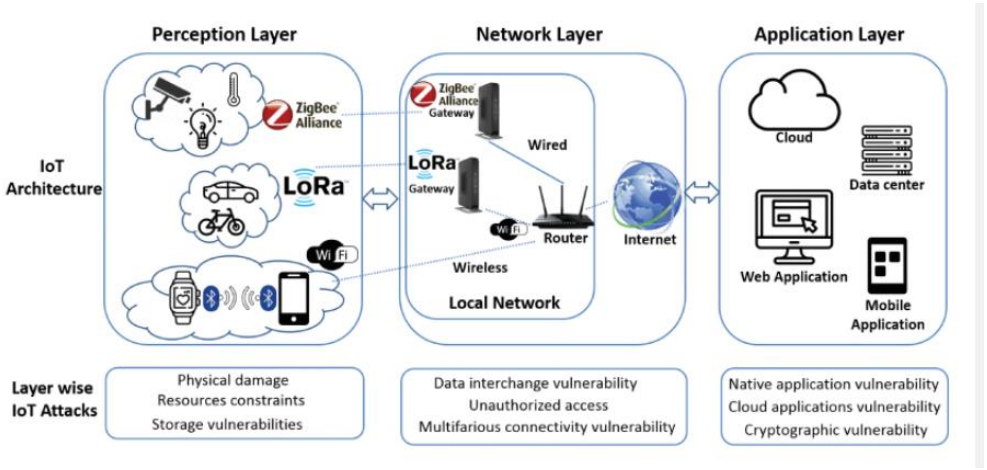


**Fig. 3** Survey Workflow [9].

As previously stated, the Internet of Things' (IoT) network layer is vulnerable to denial-of-service (DoS) assaults. Apart from denial-of-service assaults, intrusions such as traffic analysis, eavesdropping, and passive monitoring can also be used by adversaries to breach the network layer's confidentiality and privacy. Because of the devices' data exchanges and remote access methods, there is a significant probability of these assaults. Attacks by "men in the middle" have the potential to penetrate the network layer, allowing for future eavesdropping. The secure communication channel will be totally disrupted if the device's critical information is intercepted. Therefore, to avoid identity theft, the T's key exchange mechanism must be sufficiently safe to stop anyone from listening in and taking advantage of the situation.

It is true that a wide range of threat actors and attack techniques may target IoT architectures. These assaults might come from within or outside, passive or aggressive. Passive attacks gather data for upcoming penetration efforts while keeping an eye out for vulnerabilities and without interfering with IoT ecosystem functions. Active attacks interfere with the targeted IoT device's or IoT ecosystem's ability to function, interrupting or blocking it. Data accessibility, man-in-the-middle, denial-of-service, distributed denial-of-service, sniffing, eavesdropping, routing, replay spoofing, and mass node authentication are just a few examples of the various ways in which these attacks and threats might manifest themselves [10].

The application layer of the Internet of Things architecture, which serves as an interface between the network and the IoT devices, is where the smart home belongs. It also has the authority to offer various services to various applications in accordance with the data that the sensors gather. Although there are other problems, security is still the most crucial [11].

In actuality, as the intrusion structure faces a quicker rate of renewal, the current new network intrusion methods often will no longer target the physical layer, application layer, or network layer.

Literature provides a specific categorisation of these emerging attacks, where the main ones targeting the application layer include vulnerable software, phishing attacks, manipulation of unstable configurations, etc., and proposes a series of solutions to these problems. Literature adds to this move and points out the vulnerability of security mechanisms due to constraints on computing power, lack of authentication/authorization mechanisms, insecure web interfaces, transmission encryption deficiencies, and their heterogeneous nature. Intrusion methods such as DOS, DDOS, MITM, spoofing, and data leakage are also problematic.

# 3. System Analysis and Application Research

## 3.1. Sensor Identity Protection

As previously stated in the literature, smart home systems are made to function as a platform for tying together appliances, gadgets, and sensors to share data and eventually provide homeowners helpful services. Nevertheless, attacks on network security might jeopardize the dependability and integrity of the services offered by these kinds of systems. The installation of smart homes' sensors or the incorporation of smart appliances into such environments renders them susceptible to theft. An attacker can be identified by analysing the data exchanged, their location or by determining the services they are associated with. Such information may render the home resident vulnerable to a vitality attack. In light of the aforementioned state of the art, this passage intends to propose a useful and attainable approach to protect the sensors' identities and prevent foreign intrusions in two ways.

Worse still, existing sensors tend to achieve connectivity with the IoT hierarchy through the medium of Wi-Fi, which, as an open-spectrum environmental medium for wireless communication, is currently at risk of interference and intrusion. The sensors of the smart home system, on the other hand, besides transmitting data with the IoT space, come with their own function of data acquisition, including the environment of the home the owner's habits and so on. Therefore, one can try to encrypt and hide the sensors. On this basis, the method of reference can be used to operate the sensors in three stages: initialisation, hiding and communication.

### 3.1.1. Sensor initialisation

The perception layer is susceptible to three distinct security issues. The first issue pertains to the amplitude of wireless signals. The majority of signals are transmitted between IoT sensor nodes via wireless technology, and interfering waves can have an impact on their effectiveness. Another thing is that it is possible for both owners and attackers to intercept sensor nodes in IoT devices. This is because a physical assault by an attacker on IoT sensors and devices is more likely since IoT nodes are usually located in outdoor and exterior locations. It is possible for components of hardware devices to be tampered with. The third problem is that network architecture is dynamic by nature because of IoT nodes' constant movement. The sensors and RFID that make up the majority of the IoT perception layer are vulnerable to many risks and assaults because of their low computational capability, storage capacity, and battery consumption. Now it is important to improve the situation on sensors.

Sensor initialisation is the operation of setting up the sensors into the home area network, this operation defines basic parameters of the bit service as well as lays the foundation for subsequent processes. The code implementation is shown in Figure 4.

**Initialization Phase**

**Input**: $def\ Q_{ID}$: Queue of existing sensors
$C_k$: Certified Key
$S = \{s_1, s_2, \ldots, s_n\}$: home sensors
**Output**: Acknowledgements
**Begin**:
1| While ($s_k$ not Join)
2| init Private_Key $= Prv(Public_{Key(C_k)})$
3| Time : $t_{ID} = 0$
4| $Join(H)$
5| $t_{ID} = random(0, threshold)$
6| $Push(t, Q_{ID}[\,])$
7| $ID = Enc(t, C_k)$
8| $Broadcast(Ack(Enc(ID, C_k)))$
9| loop
**End**

**Fig. 4** The initialisation phase as sensors join the home area network [12].

In this, the first two or three lines are the basic information about the sensor, including the public key certificate time variable of the sensor. The fourth line starts the introduction of the algorithm with

the introduction of random numbers. The introduction of these random numbers facilitates the subsequent hiding of these sensors.

### 3.1.2. Sensor hiding

In this phase, the sensors will randomly generate time values, the identity of the sensors will be encrypted, and broadcast messages from other sensors will be obtained and need to be identified in time for subsequent updates of the sensor sequence. The implementation is shown in Fig. 5.

**Concealment Phase**

**Input**: $threshold$
$C_k$: $Certified\ Key$
**Output**: $t_{ID}, Acknowledgements$
**Begin**:
1| $t_{ID} = random(0, threshold)$
2| $ID = Enc(t_{ID}, C_k)$
3| $Broadcast(Ack(Enc(ID, C_k)))$
4| $while(receive(Ack(t_{ID}))\ \{$
5| $t_{ID} = Dec(t_{ID}, C_k)$
6| $Push(t_{ID}, Q_{ID}[\,])$
7| $send(Ack(t_{ID}))\ \}$
8| $loop$
**End**

**Fig. 5** Time-based Scrambling of Sensors IDs [12].

### 3.1.3. Sensor communication

In this phase, sensors need to sense, receive and synchronise in order to maintain the system queue. The significance of the existence of this phase lies in the fact that the large number of random numbers generated and entered into the sensor queue in the first two phases tends to lead to errors in the communication between the sensor collective and the IoT space, and this phase prevents multiple sensors from occupying the same resources through a rational ordering. Figure 6 will show the principle of this algorithm, where the module first initializes the environment and establishes a time limit. This is a universally recognized value. Sensing the surroundings and reporting the information in the form of an encrypted message is the responsibility of the first thread. Waiting for messages from nearby sensors is the responsibility of the receiving thread. Lastly, the system queue is kept up to date by the synchronization thread.

**Communication Phase**

**Input**: $threshold$
$C_k$: $Certified\ Key$
**Output**: $t_{ID}, Acknowledgements$
**Begin**:
1| $initialization\ (threshold, C_K, S)$
2| $if\ t - 1_{ID} = t_{ID}$ )
3| $t_{ID} = ranodm(0, threshold)$
4| $Thread\ Sensing$ ::
5| **begin**
6| $Sense_{ID}(m)$
7| $m = Enc(m, C_k)$
8| $Unicast(m, Q_{ID})$
9| **end**
10| $Thread\ Receiving$ ::
11| **begin**
12| $receive(m)$
13| $m = Dec(m, C_k)$
14| $sender = get_{ID}(t_{ID}, m)$
15| $get\_data(m)$
16| $process\_data(m)$
17| **end**
18| $Thread\ Synchronize$ ::
19| **begin**
20| $Scramble_{IDs}(Q_{ID})$
21| $set\_queue(Q_{ID})$
22| **end**
**End**

**Fig. 6** Main communication algorithm [12].

### 3.2. Intrusion detection system

An advanced intrusion detection system is pivotal for mitigating a range of cyberattacks in smart home environments. This study introduces a swift and effective intrusion detection algorithm, evaluated using the "DS2OS" IoT dataset, which is derived from an intelligent home context. The dataset compiles traces from diverse smart home devices like motion sensors, light controllers, and smart doors, illustrating how these devices interact. These traces are essential for identifying various threats, encompassing not only normal behavior but also cyberattacks such as DoS attacks, data probing, and spying. The paper proposes a tailored, lightweight, IDS-independent, three-layer architecture specific to smart home systems. The first layer of this system scans the network, identifies IoT devices by their MAC addresses, and categorizes them based on their network behavior. The second layer assesses packets from these devices to determine if they are malicious. Finally, the third layer classifies any detected malicious packets into one of four main attack types. The system's output, in the event of an attack, provides vital information for model training: the type of attack, the nature of the packet (malicious or benign), and the MAC address of the targeted device. This system not only differentiates between various IDS implementations but also integrates machine learning models to enhance the generation of datasets and the automatic analysis of threat levels from external signals. This framework is essential for improving the resilience of smart homes against increasingly sophisticated cyber threats.

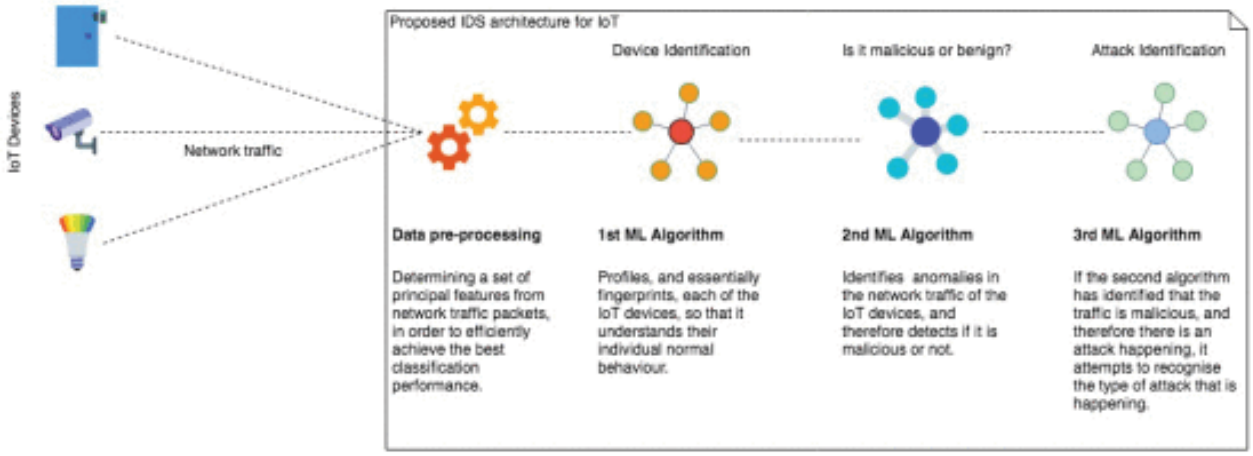


**Fig. 7** An overview of the three-layer IDS's suggested architecture[7]

## 4. Conclusion

The smart home sector has seen explosive growth with the advent of IoT technologies, infusing new vitality into home automation. However, the increased connectivity of numerous devices introduces significant risks of network intrusion, particularly because internet protocols and authentication measures remain underdeveloped. Security considerations for smart home systems have been somewhat overlooked, raising the risk of data breaches. This paper evaluates the security of smart home systems by analyzing prevalent protective and intrusive methods. It further proposes improvements to existing security measures, incorporating insights from recent advancements in Intrusion Detection Systems and other contemporary technologies. This evaluation aims to enhance understanding of the vulnerabilities within smart home systems and guide future enhancements in this rapidly evolving field.

## References

[1] Cvitić, I., Peraković, D., Periša, M., et al. (2022). An Overview of Smart Home IoT Trends and Related Cybersecurity Challenges. Mobile Networks and Applications, 2022. https://doi.org/10. 1007/ s11036 - 022-02055-w.

[2] Wang Jice, Li Yilian, Jia Yan, et al. (2018). An Overview of Smart Home Security [J]. Journal of Computer Research and Development, 55(10): 2111-2124.

[3] Ajay Kumar, K. Abhishek, M.R. Ghalib, A. Shankar, X. Cheng. (2022). Intrusion Detection and Prevention System for an IoT Environment. Digital Communications and Networks, 8(4): 540-551. https://doi.org/10.1016/j.dcan.2022.05.027.

[4] Touqeer, H., Zaman, S., Amin, R., et al. (2021). Smart Home Security: Challenges, Issues, and Solutions at Different IoT Layers. J Supercomput, 77: 14053-14089. https://doi.org/10.1007/ s11227- 021-03825-1.

[5] Albulayhi, K., Smadi, A.A., Sheldon, F.T., Abercrombie, R.K. (2021). IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors, 21(19): 6432. https://doi.org/10.3390/ s21196432.

[6] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. In IEEE Communications Surveys & Tutorials, 21(3): 2671-2701. https://doi.org/10.1109/COMST.2019.2896380.

[7] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. In IEEE Internet of Things Journal, 6(5): 9042-9053. https://doi.org/10.1109/JIOT.2019.2926365.

[8] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., Stiller, B. (2022). Landscape of IoT Security. Computer Science Review, 44: 100467. https://doi.org/10.1016/j.cosrev.2022.100467.

[9] Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I. (2015). Internet of things (IoT) security: current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST): 336-341. https://doi.org/10.1109/ICITST. 2015. 7412116.

[10] Zhu, X., Xu, H., Zhao, Z., & others. (2021). An Environmental Intrusion Detection Technology Based on WiFi. Wireless Personal Communications, 119(2), 1425-1436.

[11] Alshboul, Y., Bsoul, A.A.R., AL Zamil, M., et al. (2021). Cybersecurity of Smart Home Systems: Sensor Identity Protection. J Netw Syst Manage, 29: 22. https://doi.org/10.1007/s10922-021-09586-9.

[12] Anthi, E., Williams, L., Burnap, P. (2018). Pulse: An adaptive intrusion detection for the Internet of Things. In Living in the Internet of Things: Cybersecurity of the IoT - 2018: 1-4. https://doi. org/1049/cp.2018.0035.