Attack Detection in Smart Home IoT Networks: A Survey on Challenges, Methods and Analysis

M. Vinay Kuma Rreddy[1(✉)], Amit Lathigara[2], and Muthangi Kantha Reddy[3]

[1] RK University, Gujarat, India
muthyalavinayreddy@gmail.com
[2] Computer Engineering, RK University, Gujarat, India
amit.lathigara@rku.ac.in
[3] Shri Vishnu Engineering College for Women, Andhra Pradesh, India

Abstract. The ubiquity of Internet of Things (IoT) gadgets in smart homes has transformed our interactions with our living environments by providing never-before-seen levels of automation and convenience. However, because IoT devices are becoming possible targets for malicious attacks, this broad connectivity also poses serious security risks. Ensuring the privacy, safety, and integrity of smart home ecosystems requires prompt detection and mitigation of these threats. Data from IoT devices is gathered, pre-processed, feature engineered, labelled, and divided into training, validation, and testing sets as part of a machine learning method to threat detection in smart home IoT networks. The process of choosing and training appropriate machine learning models—which can include everything from classification techniques to anomaly detection algorithms—is crucial. Methods are surveyed to review different types of cyber-attacks, such as denial-of-service (DoS), distributed denial-of-service (DDoS), probing, user-to-root (U2R), remote-to-local (R2L), botnet attack, spoofing, and man-in-the-middle (MITM) attacks. To protect user information, data anonymization and encryption techniques are used with privacy considerations. Another strategy that has been put forth aims to improve the security of IoT networks in smart homes by providing a strong defence against new threats and equipping users with the information and resources they need to keep their connected world safe. To provide a full overview of the numerous advancements in this field, a list of all works published in the literature to date is incorporated. Lastly, the study also includes suggestions for future research directions.

Keywords: Smart Home · IoT (Internet of Things) · Attack Detection · Machine Learning · Anomaly Detection · Cybersecurity · Cyber attacks

X. Cheng (Ed): BROADNETS 2024, LNICST 601, pp. 310–319, 2025.
https://doi.org/10.1007/978-3-031-81168-5_29

1 Introduction

1.1 Background

Smart homes are among the most well-known uses of the Internet of Things (IoT), which has brought about an era of never-before-seen convenience and automation in our daily lives. A variety of networked gadgets, from voice-activated assistants and security cameras to lighting controls and thermostats, work together to create an intelligent living environment in a typical smart home. Smart homes are becoming more vulnerable to hostile cyberattacks due to their interconnection, which simultaneously brings about an intricate web of vulnerabilities and improves comfort and energy efficiency. Protecting the integrity, safety, and privacy of the inhabitants as well as their data depends critically on the security of these intricate ecosystems. A key component of this effort is attack detection in smart home IoT networks. To detect and react to malicious activity in real-time, it entails the ongoing monitoring and analysis of network traffic, device interactions, and device behaviour. Sophisticated technologies must be integrated to achieve successful attack detection, and machine learning is becoming a potent tool in this field. Protecting the integrity, safety, and privacy of the inhabitants as well as their data depends critically on the security of these intricate ecosystems [1]. A key component of this effort is attack detection in smart home IoT networks. To detect and react to malicious activity in real-time, it entails the ongoing monitoring and analysis of network traffic, device interactions, and device behavior. Sophisticated technologies must be integrated to achieve successful attack detection, and machine learning is becoming a potent tool in this field. A key component of this survey is privacy and regulatory compliance, which guarantees that user data protection is given top priority throughout the attack detection process. Furthermore, user awareness and education are emphasized as crucial elements of a comprehensive security plan, enabling locals to actively take part in upholding a safe smart home environment. In a time when lines separating virtual and real worlds are becoming increasingly blurred, smart home security becomes essential. The proposed research will enable IoT network administrators and owners of smart homes to strengthen their defences against new threats and reap the benefits of a connected home with assurance and comfort.

The standardization of security protocols and practices among various IoT devices represents a significant research gap [2]. Standardized security frameworks that can be widely implemented are desperately needed, as a wide range of manufacturers are producing devices with differing degrees of security. Through the reduction of vulnerabilities brought about by device diversity, research aimed at establishing and promoting such standards would help to create a more cohesive and secure IoT landscape. The area of user-centric security solutions for smart homes is another noteworthy research gap. There is a need to look more closely at the behavioral and psychological aspects of how people interact with smart devices, even though many studies concentrate on the technical aspects of IoT security. Designing more user-friendly and efficient security solutions can benefit from an understanding of users' perceptions of, and reactions to, security measures as well as their attitudes toward privacy. More user-friendly and intuitive security measures may result from research that closes this gap.

1.2 Types of Smart Home Attacks

The increasing interconnectedness of IoT devices and the growing dependence on digital technologies in daily life make smart homes vulnerable to various cyberattacks. Typical smart home attack types include the following:

Unauthorized Access: Brute Force Attacks: Attackers try a variety of username and password combinations until they discover the right one in an effort to access smart home devices.

Default Credentials: If homeowners don't change the default usernames and passwords that some Internet of Things devices come with, hackers might take advantage of them.

Device Vulnerabilities: Zero-Day Exploits: Vulnerabilities in IoT device firmware or software that have not yet been fixed by the manufacturer may be found and exploited by attackers. Firmware Tampering: In order to take control of or interfere with the operation of IoT devices, malevolent actors may manipulate their firmware.

Malware: IoT Malware: Smart home devices can become infected with malware made especially for Internet of Things devices, which can then turn them into bots that take part in botnet attacks. Ransomware: Data from smart home devices may be encrypted by attackers, who then demand a ransom to unlock the device, making it unusable until the ransom is paid.

Man-in-the-Middle (MitM) Attacks: Eavesdropping: Attackers monitor and intercept device-to-device communication in an attempt to obtain private information or insert nefarious commands. Session Hijacking: When a session between devices is hijacked by malicious actors, they can manipulate or listen in on the conversation.

Phishing: Phishing Emails: Attackers trick homeowners into disclosing login information or clicking on malicious links that jeopardize the security of their smart homes by sending them misleading emails or messages.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: DoS Attacks: Attackers overwhelm a system or network with excessive traffic, making it unusable or crashing it. DDoS Attacks: A target device or network is overloaded by several compromised devices, rendering it inaccessible to authorized users.

Voice Assistant Exploits: Voice Command Spoofing: Voice-activated smart devices can be tricked by attackers using voice recordings or other techniques, which could allow them to access the device without authorization. Eavesdropping: Voice assistants and smart speakers may be susceptible to illegal users listening in on them.

Physical Attacks: Device Theft: Unauthorized access to data and device control are potential outcomes of IoT device theft. Hardware Manipulation: Attackers may physically alter gadgets in an effort to take over or obtain private data.

IoT Network Attacks: Network Sniffing: To learn more about how devices communicate with one another, attackers on a local network intercept and examine data packets. Traffic Analysis: Network traffic can be used by malicious actors to obtain data about user behavior and device usage patterns.

Social Engineering: Impersonation: In order to deceive homeowners into granting access to their smart home systems, attackers may assume the identity of authorized users or service providers. Manipulating Users: persuading users to do security-compromising activities, like sharing private information or turning off security features.

To protect the integrity, privacy, and functionality of smart home environments, homeowners and IoT device manufacturers must have a thorough understanding of these types of smart home attacks and implement strong security measures.

1.3 Major Challenges of Smart Home Attacks

The intricacy and variety of linked devices in smart homes and IoT networks create many obstacles for security professionals to overcome. Among the principal difficulties are:

- Device Diversity: A variety of devices from various manufacturers are included in smart homes, each with unique security features and vulnerabilities. It's difficult to secure and manage this diverse ecosystem [3].
- Lack of Standardization: Inconsistencies in security measures and unaddressed vulnerabilities can result from a lack of standardization in security protocols and practices amongst IoT devices.
- Weak Authorization and Authentication: A lot of Internet of Things (IoT) devices have weak or default authentication systems, which leaves them open to brute force attacks and unauthorized access.
- Firmware Updates: It can be difficult to guarantee that every device is consistently updated with the most recent firmware patches, particularly when certain devices do not have automated update systems in place.
- Resource Constraints: IoT devices frequently have limited computational resources, which makes it difficult to implement strong security measures without negatively impacting device performance [4]. This is known as resource constraints.
- Privacy Issues: Data collection by Internet of Things devices may give rise to privacy issues. It's always difficult to strike a balance between user privacy and data collection for functionality.
- Network security: It's critical to protect device-to-central hub or cloud server communication. The network as a whole may be compromised by shoddy encryption or unsafe communication methods.
- Physical Security: Unauthorized access or data breaches can result from physical tampering with IoT devices. It can be difficult to ensure physical security, particularly for remote or outdoor devices [5].
- Vendor Accountability: It can be difficult to hold IoT device makers responsible for security flaws and to make sure they offer prompt updates and support.
- User Awareness: A lot of people who use smart homes might not know about security best practices or might forget to update their default credentials, leaving them open to attacks.
- Legacy Devices: Antiquated Internet of Things gadgets might not be updated or supported, making them always open to known vulnerabilities.

- Interoperability: It can be challenging to make sure that various IoT devices can coexist peacefully while still maintaining security.
- Complicated Attack Surfaces: A large attack surface is produced by the networked structure of smart homes. If one device is compromised, an attacker may be able to use it as a springboard to target other devices.
- Machine learning for threat detection: Although it can improve security, there are drawbacks, including the need to adjust to changing attack strategies and deal with false positives.
- Regulatory Adherence: Respecting privacy and security laws can be difficult, particularly when it comes to information gathered by Internet of Things devices.
- IoT Botnets: The advent of Internet of Things (IoT) botnets, which utilize compromised devices to launch extensive attacks, presents a formidable obstacle to network security [6].
- User Behavior: It can be difficult to distinguish between benign user behavior and malevolent activity, particularly when insider threats are involved.

A multifaceted strategy including device makers, network administrators, users, and regulatory agencies is needed to address these issues. It entails putting strong security measures in place, training users, encouraging cooperation among stakeholders, and remaining alert in the face of changing threats.

1.4 Research Goals

Research goals for an IoT network and smart home security study should be in line with filling in the identified knowledge gaps and resolving the issue. The following are a few research goals:

- Create uniform security frameworks: To create best practices and standardized security protocols that can be used with a variety of IoT devices, improving interoperability and lowering vulnerabilities caused by device diversity.
- Enhance Security with a focus on users: To conduct research on user behaviors, attitudes, and preferences related to smart home security and to develop user-friendly, intuitive security solutions that meet user expectations.
- Examine Legacy Device Security: To guarantee the continuous security of smart home ecosystems, evaluate the security of older IoT devices that might not have received updates and investigate methods to reduce vulnerabilities in legacy devices.
- Proactive Threat Mitigation: The aim of proactive threat mitigation is to investigate new threats in smart home environments, create threat intelligence systems, and investigate predictive analytics in order to prevent threats before they arise.
- Privacy-Preserving Solutions: Investigate methods and tools, like data anonymization, encryption, and user-controlled data sharing, that protect user privacy in smart home settings.
- User Authentication and Access Control: The aim of this study is to create strong user authentication methods and access control techniques that guard against unwanted access to smart home systems and gadgets.

These research goals take into account the complex interplay between IoT networks and smart home security, tackling various facets of the problem statement and advancing

the creation of all-encompassing, efficient, and user-focused security solutions for smart home ecosystems.

2 Related Work

The related work included a variety of IoT-related studies on intrusion detection systems. This section was created using the proposals submitted between 2020 and 2023 and was funded by research articles that could be found in the scientific repository (ACM Digital Library, Springer Link, Google Scholar, IEEE Xplore, and Science Direct). Exposure to the works pertaining to the designated topic is provided by this production. Regarding the security issues with layers, an overview of various proposed research works is presented. According to the IoT layer structure, Table 1 shows the work that has been done thus far on security issues and mitigation strategies.

2.1 Artificial Intelligence (AI) Methods Used for Smart Home Attack Detection

Several Deep Learning (DL) and Machine Learning (ML) models are employed in the detection of Smart Home attacks. In order to increase attack detection accuracy and automate IoT device communication, ML and DL have been applied to smart home attack detection. These methods can assist in identifying patterns that are not readily apparent to the human eye and have been used to analyze a variety of attack patterns.

- Convolutional Neural Networks (CNNs): Deep learning models, such as CNNs, are frequently employed in the analysis of smart home attacks. They have been applied to the classification of various types of attacks and traffic patterns. CNNs have the benefit of automatically identifying features from the traffic, which eliminates the need for human feature engineering [31].
- Random Forest (RF): A popular machine learning model called RF is used to classify smart home attacks according to their traffic rules. It is utilized in many regression and classification problems. It has been demonstrated that RF is useful for both identifying smart home intrusions and distinguishing between typical and unusual traffic.
- Support Vector Machine (SVM): SVM is a supervised learning model with applications in regression analysis, outlier identification, and classification. Using the features that are taken out of the different kinds of traffic, it has been used to classify traffic patterns in smart home attack detection.
- Recurrent Neural Networks (RNNs): Time series data and other sequential data have been analyzed using RNNs, a type of DL model. RNNs have been used to examine traffic pattern sequences in order to monitor an attack's evolution over time [32].
- Generative Adversarial Networks (GANs): One kind of DL model that can be used to create new images is a GAN. Other DL models can be trained using the synthetic attacks that GANs have produced on Internet of Things smart homes [33].
- Hybrid models: To enhance the effectiveness of smart home attack detection, researchers have put forth a number of hybrid models that combine the best features of various models. As an illustration, consider combining CNNs with RF or CNNs with SVM.

Table 1. Comparison of existing solutions on Smart Home IoT security issues

Author	Area	Application	Techniques	Data Used	Accuracy	Remarks
Fernando H. Y. et.al. [7]	IoT Network	Attack Detection	CluStream and Page-Hinkley Test	publicly available datasets	97%	Different types of attacks were detected with the precision stayed above 87%
Chenxu Jiang et.al. [8]	IoT Network	Anomaly Detection	Innovative metric to quantify the temporal similarity	real-world testbed	93%	Delay-caused anomalies are detected
J. Araya et.al. [9]	Smart Home IoT Network	Anomaly-based cyberattacks detection	Ensemble and deep learning techniques	publicly available datasets	NA	Survey has been done
Ramesh Paudel et.al. [10]	Smart Home IoT Network	Detecting DoS Attack	Graph-Based Approach	real-world data collected from IoT-equipped smart home	92%	It outperforms current graph-stream anomaly detection approaches
A.V. Chandak et.al. [11]	Smart Home IoT Network	DDoS attack detection	Feature Selection SVM (FSSVM)	DDoS dataset	93%	FSSVM algorithm provides better accuracy compared to KPCA-SVM, SVM, and Naive Bayes algorithms
Soe YN, Feng et. Al. [12]	IoT network	IoT Botnet Attack Detection	ANN, J48 decision tree, NB	N-BaIoT	99.10	Hybrid sequential detection scheme is proposed using feature selection with ML algorithms
Churcher A et. Al. [13]	IoT Networks	IoT Attack Classification	KNN, SVM,DT,NB,RF,LR	Bot-IoT dataset	KNN- 99.32 (Multi class) ANN – 99.47 (Binary Class)	For weighted and Non Weighted datasets in multi classification ANN and KNN are very accurate and for binary classification ANN achieves high accuracy
Lima Filho et. Al. [14]	IoT Network	DoS/DDoS Attack Detection	AdaBoost, RF, DT, LR, SGD	CICIDS2017, CSE-CIC-IDS2018	RF – 99.93	RF achieved highest accuracy with 20 feature and 28 feature dataset
M. Shafiq et. Al. [15]		Malicious Bot-IoT Traffic Detection	Corrauc algorithm	Bot-IoT Data Set	99.12	C 4.5 DT and RF provides high acuuracy
Shafiq et. Al. [16]	Smart City	Bot-IoT attacks traffic identification	Bijective soft set algorithm, NB, DT, RF	Bot-IoT Data Set	BayesNet-99.77 C4.5–99.99	
Tuan et. Al. [18]	Network Traffic	Botnet DDoS attack detection	SVM,DT,NB,ANN, USML(Unsupervised Learning)	UNBS-NB-15 KDD99	98.08	Unsupervised Learning model provides highest accuracy
I.Alrashdi et. Al. [19]	Smart City	Anomaly Detection	RF	UNBS-NB-15	99.34%	

(*continued*)

Table 1. (*continued*)

Author	Area	Application	Techniques	Data Used	Accuracy	Remarks
Abu Al-Haija et. Al. [20]	IoT Communication Networks	Detection and Classification of Cyber-Attacks	CNN	NSL-KDD	99.3%	Research is done using 2 class and 5 class label. Among this 2 class label gives highest accuracy
Gaber, T. et. Al. [21]	smart IoT applications	Injection attack detection	SVM, RF, DT	AWID	99%	In this research they used 76, 13 and 8 features
Almaraz-Rivera et. Al. [22]	IoT Devices	Transport and Application Layer DDoS Attacks Detection	RF, DT, RNN, MLP, LSTM, GRU	Bot-IoT Dataset	99.94 99.97	
Abu Al-Haija et. Al. [24]	IoT Networks	Botnet Attack Detection	AdaBoost, RUSBoost, ELBA-IoT	N-BaIoT-2021	99.6%	
Gaur, V et. Al. [25]	IoT Devices	Early Detection of DDoS Attacks	RF,DT, KNN, XGBoost	CICDDoS2019	98.34%	ANOVA feature selection method for XGBoost gives highest accuracy
Albulayhi K et. Al. [26]	IoT Networks	IoT Intrusion Detection	Bagging, MLP, J48, IBk	IoTID20 NSL-KDD	99.7	Intersection theory with ensemble gives higesh accuracy
Salman, O et. Al. [27]	IoT device	abnormal traffic detection	DT,RF RNN, ConvNet	Own Testbed	99.93	RF gives highest Accuracy. Data is balanced
Anthi, E et. Al [30]	smart home networks	denial of service attack defence	RF, J48 DT, SVM	testbed	99.99	

It's crucial to remember that these models are complementary instruments that can be applied to obtain the best outcomes for a particular situation rather than antagonistic ones. Additionally, as these models are still in the early stages of development, more validation across larger datasets and in clinical settings are required to guarantee their generalizability and dependability.

3 Conclusion

In conclusion, with our world becoming more interconnected, the fields of IoT networks and smart home security are critical. This review of the literature emphasizes how diverse the field's research is, addressing everything from user-centric security and proactive threat mitigation to the vulnerabilities of Internet of Things devices and emerging cyber threats. It emphasizes how important it is to have user-friendly security solutions, standardized security procedures, and legacy device security tactics. It also highlights how crucial it is to comprehend how physical and digital security intersect in smart homes, as well as how important privacy protection, authentication, and access control are. This work presents a thorough summary of the state of the art, offering insightful analysis and helpful recommendations for handling the intricate problems associated with smart home security.

References

1. Ai, Y., Peng, M., Zhang, K.: Edge computing technologies for internet of things: a primer. Digital Commun. Netw. **4**(2), 77–86 (2018)
2. Alduailij, M., Khan, Q.W., Tahir, M., Sardaraz, M., Alduailij, M., Malik, F.: Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. Symmetry. **14**(6), 1095 (2022)
3. Shorey, T., Subbaiah, D., Goyal, A., Sakxena, A., Mishra, A.K.: Performance comparison and analysis of Slowloris, GoldenEye and Xerxes DDoS Attack Tools. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, pp. 318–322 (2018)
4. Mishra, A., Cheng, A.M.K., Zhang, Y.: Intrusion detection using principal component analysis and support vector machines. In: 2020 IEEE 16th International Conference on Control Automation (ICCA). IEEE, pp. 907–912 (2020)
5. Jan, S.U., Ahmed, S., Shakhov, V., Koo, I.: Toward a lightweight intrusion detection system for the internet of things. IEEE Access. **7**, 42450–42471 (2019)
6. Chi, H., Fu, C., Zeng, Q., Du, X.: Delay wreaks havoc on your smart home: delay- based: automation interference attacks. In: IEEE Symposium on Security and Privacy (S&P), IEEE Computer Society, p. 1575 (2022)
7. Fernando, H.Y., Nakagawa, et al.: Attack detection in smart home IoT networks using CluStream and Page-Hinkley test. In: 2021, IEEE Latin-American Conference on Communications (LATINCOM) (2021)
8. Jiang, C., et al.: Effective anomaly detection in smart home by integrating event time intervals. Elsevier Procedia Comput. Sci. **210**, 53–60 (2022)
9. Araya, J., et al.: Anomaly-based cyberattacks detection for smart homes: a systematic literature review. Elsevier, Internet of Things **22** (2023)
10. Ramesh, P., et al.: Detecting DoS attack in smart home IoT devices using a graph-based approach. In: IEEE International Conference on Big Data (Big Data) (2019)
11. Ashish, V.C., et.al.: DDoS attack detection in smart home applications. J. Software Pract. Exper. Wiley (2023)
12. Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R., Sakurai, K.: Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors **20**(16), 4372 (2020). https://doi.org/10.3390/s20164372
13. Churcher A, et al.: An experimental analysis of attack classification using machine learning in IoT networks. Sensors **21**(2), 446 (2021). https://doi.org/10.3390/s21020446
14. Lima Filho, F.S.D., Silveira, F.A., de Medeiros Brito Junior, A., Vargas-Solar, G., Silveira, L.F.: Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Secur. Commun. Netw. 1–15 (2019)
15. Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M.: CorrAUC: a Malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques. In: IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242–3254, 1 March 2021. https://doi.org/10.1109/JIOT.2020.3002255
16. Shafiq, M., Tian, Z., Sun, Y., Du, X., Guizani, M.: Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Futur. Gener. Comput. Syst. **107**, 433–442 (2020)
17. Al-Shareeda, M.A., Manickam, S., Saare, M.A.: DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison (December 16, 2022). Bull. Electr. Eng. Inf. **12**(2), 930–939 (2023).SSRN: https://ssrn.com/abstract=4515135
18. Tuan, T.A., Long, H.V., Son, L.H., et al.: Performance evaluation of Botnet DDoS attack detection using machine learning. Evol. Intel. **13**, 283–294 (2020). https://doi.org/10.1007/s12065-019-00310-w

19. Alrashdi, I., et al.: IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas, NV, USA **2019**, 0305–0310 (2019). https://doi.org/10.1109/CCWC.2019.8666450
20. Abu Al-Haija, Q., Zein-Sabatto, S.: An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics **9**(12), 2152 (2020). https://doi.org/10.3390/electronics9122152
21. Gaber, T., El-Ghamry, A., Hassanien, A.E.: Injection attack detection using machine learning for smart IoT applications. Phys. Commun. **52**, 101685 (2022)
22. Almaraz-Rivera, J.G., Perez-Diaz, J.A., Cantoral-Ceballos, J.A.: Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models. Sensors **22**(9), 3367 (2022)
23. Inayat, U., Zia, M.F., Mahmood, S., Khalid, H.M., Benbouzid, M.: Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects. Electronics **11**(9), 1502 (2022)
24. Abu Al-Haija, Q., Al-Dala'ien, M.: ELBA-IoT: an ensemble learning model for botnet attack detection in IoT networks. J. Sens. Actuat. Netw. **11**(1), 18 (2022). https://doi.org/10.3390/jsan11010018
25. Gaur, V., Kumar, R.: Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arab. J. Sci. Eng. **47**(2), 1353–1374 (2022)
26. Albulayhi, K., Abu Al-Haija, Q., Alsuhibany, S.A., Jillepalli, A.A., Ashrafuzzaman, M., Sheldon, F.T.: IoT intrusion detection using machine learning with a novel high performing feature selection method. Appl. Sci. **12**(10), 5015 (2022). https://doi.org/10.3390/app12105015
27. Salman, O., Elhajj, I.H., Chehab, A., Kayssi, A.: A machine learning based framework for IoT device identification and abnormal traffic detection. Trans. Emerg. Telecommun. Technol. **33**(3), e3743 (2022)
28. Abu Al-Haija, Q., Krichen, M., Abu, E.W.: Machine-learning-based darknet traffic detection system for IoT applications. Electronics **11**(4), 556 (2022). https://doi.org/10.3390/electronics11040556
29. Touqeer, H., Zaman, S., Amin, R., et al.: Smart home security: challenges, issues and solutions at different IoT layers. J. Supercomput. **77**, 14053–14089 (2021). https://doi.org/10.1007/s11227-021-03825-1
30. Anthi, E., Williams, L., Javed, A., Burnap, P.: Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. Comput. Secur. **108**, 102352 (2021)
31. Bang, A.O., Rao, U.P.: A novel decentralized security architecture against sybil attack in RPL-based IoT networks: a focus on smart home use case. J. Supercomput. **77**, 13703–13738 (2021). https://doi.org/10.1007/s11227-021-03816-2
32. Kumar, P., Chouhan, L.: A secure authentication scheme for IoT application in smart home. Peer-to-Peer Netw. Appl. **14**, 420–438 (2021)
33. Alshboul, Y., Bsoul, A.A.R., AL Zamil, M., et al.: Cybersecurity of smart home systems: sensor identity protection. J. Netw. Syst. Manage. **29**, 22 (2021). https://doi.org/10.1007/s10922-021-09586-9